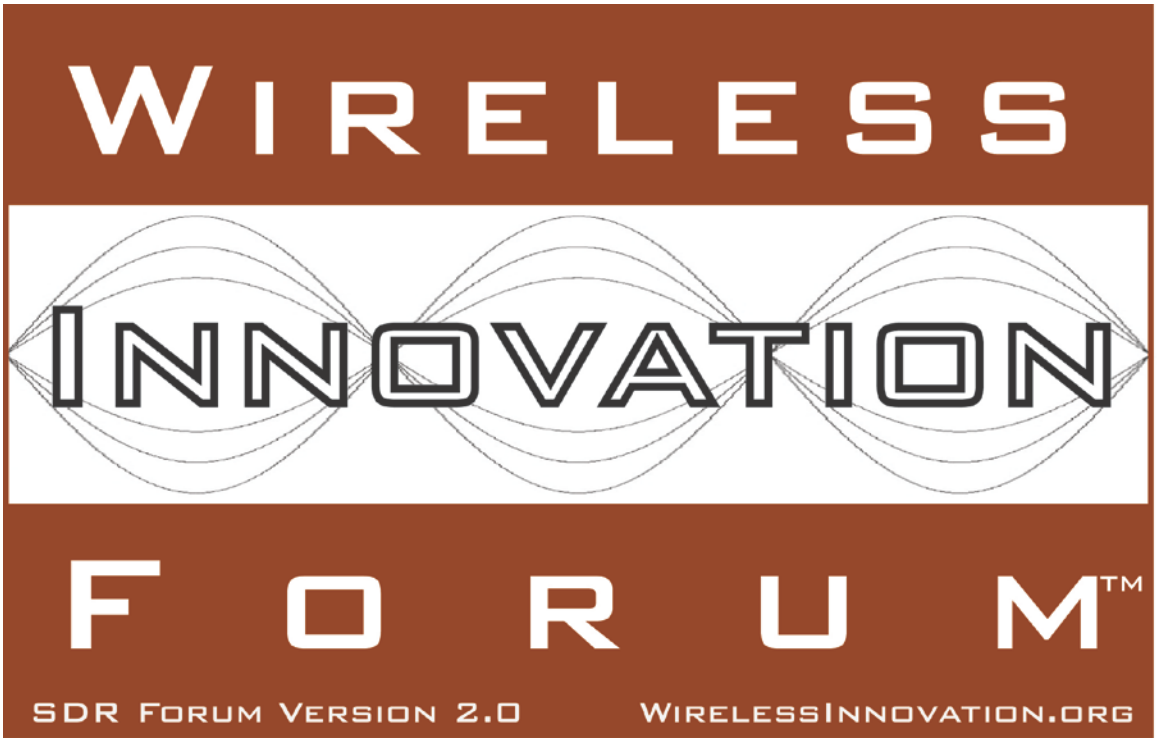

Use Cases for Cognitive Applications in Public Safety Communications Systems Volume 2: Chemical Plant Explosion Scenario

Document WINNF-09-P-0015-V1.0.1

Version 1.0.1
26 January 2010

TERMS, CONDITIONS & NOTICES

This document has been prepared by the Public Safety Special Interest Group to assist The Software Defined Radio Forum Inc. (or its successors or assigns, hereafter "the Forum"). It may be amended or withdrawn at a later time and it is not binding on any member of the Forum or of the Public Safety Special Interest Group.

Contributors to this document that have submitted copyrighted materials (the Submission) to the Forum for use in this document retain copyright ownership of their original work, while at the same time granting the Forum a non-exclusive, irrevocable, worldwide, perpetual, royalty-free license under the Submitter's copyrights in the Submission to reproduce, distribute, publish, display, perform, and create derivative works of the Submission based on that original work for the purpose of developing this document under the Forum's own copyright.

Permission is granted to the Forum's participants to copy any portion of this document for legitimate purposes of the Forum. Copying for monetary gain or for other non-Forum related purposes is prohibited.

THIS DOCUMENT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS DOCUMENT.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the specification set forth in this document, and to provide supporting documentation.

Wireless Innovation Forum ™ and SDR Forum ™ are trademarks of the Software Defined Radio Forum Inc.

ACKNOWLEDGEMENTS

This document was drafted by the Public Safety Special Interest Group of the Wireless Innovation Forum (SDR Forum version 2.0). In addition, inputs were provided by members of the National Institute of Justice Communications Technology Working Group. Their contributions were significant and gratefully appreciated.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Cognitive radio can be thought of as a radio or network of radios that automatically adjust its behavior or operations to achieve desired objectives[1]; the key take away is that cognitive radios can enable a network that can make real-time adjustments, with little or no human intervention. This technology is already used in military and commercial communications networks. This report, the second in a series of reports written by the Wireless Innovation Forum, highlights how such capabilities, residing in radios or implemented in a network, can improve the communications of public safety first responders.

The objective of this report is to provide:

- **Researchers and system developers** with an understanding of desired cognitive capabilities, from which technical requirements and specifications can be derived;
- **Public safety agencies** with an understanding of the potential value of cognitive radio technology and an understanding of policy and procedural changes that may be required to fully utilize evolving cognitive radio technology and regulatory changes.
- **Regulatory agencies** with an understanding of the regulatory issues and identification of potential changes that may be required to fully utilize evolving cognitive radio technology to benefit public safety.

This report outlines a hypothetical scenario of a major explosion at a chemical plant in a mid-sized metropolitan area. The scenario was developed with input from public safety practitioners, communications system engineers, and radio developers. It provides the basis (events, activities, and timelines) required to analyze the impact of cognitive-based radio and network functions on first responder communications and mission effectiveness. Based on the analysis, we conclude that the utilization of cognitive radio functions can dramatically increase the ability of Incident Commanders to meet their mission objectives.

The report provides eight examples (defined as use cases) of how cognitive radio or network technology could be utilized, and explains in detail the technical, regulatory, and operational procedure developments required to make these capabilities available for public safety use.

This report showcases the potential for improving first responders' communications capabilities through the application of cognitive functionality. The tailoring of wireless networks to meet varied incident requirements, enhance interoperability, improve system performance and manage scarce spectrum resource management are the functions of note for the stakeholder(s), and allow the communications capabilities to adjust dynamically as an incident evolves. First responders can be confident that critical information will flow as needed despite changes in coverage, connectivity, and loading on communications systems.

[1] Software Defined Radio Forum, *SDRF Cognitive Radio Definitions*. SDR Forum Report SDRF-06-R-0011, available at www.wirelessinnovationforum.org.

1 Introduction

The maturing of software defined radio technology, when combined with evolving concepts of cognitive radio technology, holds great promise for public safety communications. In a report released in 2006, the Public Safety Special Interest Group (SIG) of the Wireless Innovation Forum (SDR Forum Version 2.0) identified potential benefits of software defined and cognitive technology to public safety.[2] One key area of interest defined in that report is cognitive applications. As a result of that initial study, the Public Safety SIG began an in-depth analysis of how cognitive technology can benefit public safety.

This report is the second in a series of reports authored by the Forum, to develop and convey concepts for the application of cognitive radio technology to enhance the communications capabilities of public safety first responders. The purpose of this series of documents is to explore in greater detail specific examples of how cognitive applications can be used in public safety communications networks to enhance emergency communications capabilities.

The objectives of the Public Safety SIG in generating this series of documents are as follows:

1. Provide **researchers and system developers** with an understanding of the desired cognitive and related functional capabilities, from which technical requirements and specifications can be derived;
2. Provide **regulatory agencies** with an understanding of the type of regulatory issues, and identification of potential changes that may be required to fully utilize evolving cognitive radio technology for the benefit public safety; and
3. Provide **public safety agencies** with an understanding of the potential value of cognitive radio technology and an understanding of the types of policy, procedural, and regulatory changes which may be required prior to deployment of this radio technology.

1.1 The Wireless Innovation Forum Public Safety Special Interest Group

The Software Defined Radio Forum Inc., doing business as the Wireless Innovation Forum, is an open, non-profit corporation dedicated to supporting the development, deployment, and use of open architectures for advanced wireless systems, with a mission to accelerate the proliferation of software defined radio (SDR), cognitive radio (CR) and dynamic spectrum access (DSA) technologies in wireless networks to support the needs of civil, commercial, and military market sectors[3].

---

[2] SDR Forum, *Software Defined Radio Technology for Public Safety*, Software Defined Radio Forum Report SDRF-06-A-0001-0.0, 14 April 2006, available at www.wirelessinnovation.org.

[3] In 2009 the Forum underwent a major strategy review, led by representatives from multiple member organizations. The result was a revised strategic plan that included rebranding the organization as the Wireless Innovation Forum (SDR Forum Version 2.0). This change in name reflects the fact that member organizations within the Forum are driving innovation in areas beyond "Software Defined Radio" to include system of systems, ad-hoc networks, cognitive radio, dynamic spectrum access, etc. The strategy update, including the name change, was put before the members by the Board of Directors at the Annual Meeting of the members on 3 December 2009 where it was approved. The legal name of the organization remains "The Software Defined Radio Forum Incorporated".

The press release announcing the name change can be found here:
http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20091203006419&newsLang=en

Activities focus on:

- Developing requirements and/or standards for reconfigurable radio technologies, to include working in liaison with other organizations to ensure that Forum recommendations are easily adapted to existing standards and evolving wireless systems
- Cooperatively addressing the global regulatory environment
- Providing a common ground to codify global developments,
- Serving as an industry meeting place

The Public Safety Special Interest Group is one of several special interest groups within the Forum that bring together developers, users, regulators, and educators to address issues specific to the application of advanced wireless technology within a particular domain or market area. Goals of the Public Safety SIG are to interface with the public safety community (including both users and vendors), to raise awareness of advanced wireless technologies, to publicize the activities of the Forum in addressing those issues, and to increase participation of the public safety community in the Forum. The Public Safety SIG also interacts with other committees and working groups within the Forum to provide the public safety community's inputs into the publications and initiatives undertaken by the Forum. In the case of this report, members of the Forum's Security and Cognitive Radio Working Groups have participated in the preparation of this report. The Public Safety SIG is a unique venue, because participation in the SIG has historically included public safety organizations, land mobile radio vendors, manufacturers of SDR for military applications, software developers, researchers, and regulators.

1.2 Document Overview

The methodology for developing cognitive use cases is based on analysis of response to actual or hypothesized events. This report is based on a hypothetical scenario of a chemical plant scenario, with events drawn from a number of sources including the chemical plant explosion scenario developed as part of the Project SAFECOM Public Safety Communications Statement of Requirements, and analysis of actual events such as the fire at a hazardous waste transfer plant in Apex, NC, in October 2006.

The background and assumptions of our analysis are provided in Section 2. In Section 3, we provide an overview of the methodology to be used throughout this series of documents. The scenario itself is presented in Section 4. Section 5 includes a discussion of cognitive radio technology use cases. Section 6 includes discussion of issues, such as security, that apply across multiple use cases defined in Section 5. The report concludes with a summary in Section 7.

2 Background and Assumptions

As noted in the Introductory Section, the potential value of cognitive radio capabilities for public safety has already been identified. In the Report on *Software Defined Radio Technology for Public Safety*[4], and based on subsequent work, the following potential observations were made about the potential impact of cognitive radio capabilities for public safety:

1. First responders can better focus on the incident/threat by eliminating manual radio operations ranging from routine to complex through the use of cognitive radio applications to:
   a. Understand the local RF environment (e.g., vicinity of public safety incident);
   b. Detect available and authorized RF resources;
   c. Decide how to best operate within the existing infrastructure/network;
   d. Use geolocation, spectrum, and network awareness to minimize interference;
   e. Automatically reconfigure radio equipment and connect to networks and other radios as needed; and
   f. Learn how to perform these steps better the next time.
2. Cognitive radio technology will enable a broad range of RF techniques that will improve performance, interoperability, and efficiency.
3. Cognitive radio technology is rapidly becoming a significant concept for *all* future communications systems and devices for two fundamental reasons:
   a. It enhances spectrum efficiency and improves user access by automatically making dynamic channel assignments, taking specialized measures to avoid harmful interference to others, and optimizing channel utilization.
   b. It enables "intelligent" self-configuring, auto-adapting systems and devices that will handle the growth trend of complex waveforms and user requirements.
4. Public Safety must carefully balance spectrum efficiency benefits against the critical need for system reliability, robustness, security, "instant on," and other application-specific requirements of the first responder.

This report documents the efforts of the Public Safety SIG to explore and analyze the potential value of cognitive radio applications to public safety.

2.1 Cognitive Radio Technology

Cognitive radio technology (note definitions in the box that follows) is rapidly evolving as a significant driver for emerging capabilities in advanced radio systems. Initial capabilities to adapt by selecting frequencies automatically to prevent interference to legacy radio systems was successfully field-demonstrated under the Defense Advanced Research Projects Agency (DARPA) XG radio program in August, 2006.[5] Demonstrations at the 2007 and 2008 DySPAN Conferences included real-time spectrum sensing/monitoring, secondary spectrum use by cooperating cognitive radios,

[4] Ibid. Section 4.3 Role of Cognitive Applications.
[5] Seeling, Frederick W., *A Description of the August 2006 XG Demonstrations at Fort A.P. Hill,* Proceedings of the IEEE Conference on Dynamic Spectrum Access Networks (DySPAN), April, 2007.

integrated policy engines, and cognitive radio development platforms.[6] Such demonstrations indicate that these basic capabilities are achievable for public safety in the near term. We recognize that from these building blocks it will still be necessary to continue development of functional capabilities that will not only work with existing radio systems but that are also proven under field conditions before such capabilities can be adopted for public safety use.

We also recognize that there are major issues that must be addressed before realizing the potential of cognitive radio technology. For example, one of the challenges in dynamic spectrum access is the hidden node problem—assuming that a frequency can be utilized when in fact it is already in use by a transmitter or receiver "hidden" (electromagnetically) from the cognitive radio. Another important issue is that cognitive capabilities assume some level of automatic reconfigurability of the radio which could have implications on the size, weight, and/or power requirements of a portable public safety radio. While not discounting the significance of these challenges, progress to date in this field suggests that they can be resolved to a level sufficient to realize the use cases outlined in this document.

[6] A summary of each of the demonstrated capabilities from the 2008 conference is available at http://cms.comsoc.org/eprise/main/SiteGen/DYSPAN_2008/Content/Home/demonstrations.html.

Definitions

(from *SDRF Cognitive Radio Definitions*. SDR Forum Report SDRF-06-R-0011)

- **Radio**: (a) Technology for wirelessly transmitting or receiving electromagnetic radiation to facilitate transfer of information. (b) System or device incorporating technology as defined in (a). (c) A general term applied to the use of radio waves—from ITU-R Radio Regulations, Article 1 (Terms and Definitions, Section 1.4).
- **Software Defined Radio**: *Radio* in which some or all of the *physical layer* functions are *Software Defined.*
- **Software Defined**: Software defined refers to the use of software processing within the radio system or device to implement operating (but not control) functions.
- **Adaptive Radio**: Radio in which communications systems have a means of monitoring their own performance and a means of varying their own parameters by closed-loop action to improve their performance.
- **Cognitive Capability**: (not defined in *SDRF Cognitive Radio Definitions*. SDR Forum Report SDRF-06-R-0011) Capabilities associated with cognitive radio, but unspecified in terms of how or where the capabilities are implemented. Note—we use this tem to reflect functionality without implying whether the capability is implemented in a subscriber radio, network, or distributed across both.
- **Cognitive Node:**
  - (Not defined in *SDRF Cognitive Radio Definitions*. SDR Forum Report SDRF-06-R-0011) A network node that has cognitive capabilities.
- **Cognitive Radio**:
  - *a) Radio* in which communication systems are aware of their environment and internal state and can make decisions about their radio operating behavior based on that information. The environmental information may or may not include location information related to communication systems.
  - b) *Radio* (as defined in a.) that utilizes *Software Defined Radio*, *Adaptive Radio*, and other technologies to automatically adjust its behavior or operations to achieve desired objectives
- **Cognitive Network**: A cognitive network is a network able to establish links between its *Cognitive Radio Nodes* to provide connectivity and to adjust its connectivity to adapt to changes in topology, operating conditions, or user needs. A cognitive network consists of nodes that are cognitive radios. In such a network, the cognitive abilities of the radio nodes include awareness of the network environment, network state and topology, and shared awareness obtained by exchanging information with neighboring nodes or other network accessible information sources. Cognitive decision making considers this collective information and is performed in coordination and/or collaboration with other nodes.
- **Public safety**: the function of safeguarding the lives and property of the general population.
- **First responder:** an individual from a police department, fire department, emergency medical team, or other similar organization. His/her responsibilities when responding to an incident are to take necessary action to save lives, protect the welfare of others, and inform other personnel of any potential danger at the scene of an incident.
  - Often the terms “first responder,” “emergency services,” and “public safety” are used interchangeably. These terms generally refer to the same group of people and functions. We use the term “public safety” in this report, but in the International Telecommunication Union (ITU) and in many parts of the world, the phrase “public protection and disaster relief (PPDR)” is the agreed terminology. For convenience, we have used the term public safety consistently throughout the report, but the acronym “PPDR” could be substituted in all occurrences without changing the meaning of the text or the objectives of the report.

2.2 Assumptions

The analysis of the scenarios described in this document, and the conclusions that are drawn in Section 7, are based on the following assumptions.

1. We derive functional capabilities from identified use cases for enhanced communications capability. We recognize that the technology to realize these use cases is generally not available in current public safety radio systems. In fact, the capabilities envisioned in this document range from those that currently exist in some types of radios (but have not generally been implemented in public safety radios) to other capabilities that may require additional research & development. While attempting to be forward-looking we also limited the scope of capabilities to those that could be reasonably achieved with extensions of technology that is at least in the research stage.

2. As noted above, cognitive capabilities defined in the following use cases include technologies that have yet to be fully developed, and as such, the cost of implementing proposed capabilities is not addressed explicitly. The Public Safety SIG has developed cost models for analyzing the cost-benefit tradeoffs of proposed SDR and cognitive capabilities[7]. These cost models, upon completion, can be applied to the functional capabilities identified in this document to support further analysis of the cost implications and tradeoffs associated with implementation of the identified capabilities.

3. The proposed use cases are not limited by existing regulatory regimes. We have attempted to be realistic in what regulatory changes are feasible. But also, given a compelling use case for public safety, we assume that the regulatory community would consider appropriate changes to existing rules, so "feasibility" is not defined in terms of current thinking but rather in terms of the use cases defined in this document. Thus for each use case documented in this report, we also identify regulatory issues that may need to be addressed. We also note that regulatory perspectives differ by country and world region; therefore adoption of regulatory changes identified in this document will vary by location.

4. In general we use the term "cognitive capabilities" in this document to reinforce the concept that the cognition required to support public safety communications is not likely to fully reside in a single radio or device. More likely, cognitive capabilities that (a) collect information about the RF environment, (b) make decisions about how to enhance communications capability, and (c) reconfigure infrastructure and subscriber equipment, will be distributed throughout multiple nodes within a public safety communications system.

5. Many of the circumstances described in the scenario in Section 4 can be addressed through deployment of additional communications capabilities that do not involve cognitive capabilities. If all events are known a priori, non-cognitive solutions can be implemented to account for those events. However, major incidents and disasters are often characterized by circumstances that are beyond the scope of planning; in addition, fiscal realities preclude implementation of contingencies for all possible situations. The real power of cognitive capabilities is to rapidly adjust to changes in the operating environment in order to maintain communications in the face of dynamic and often unanticipated circumstances. Thus we as-

[7] SDR Forum, "Public Safety SDR Lifecycle Cost Estimation Workbook," Report No. SDRF-09-P-0001-V1.0.0, available at http://www.sdrforum.org/pages/documentLibrary/documents/SDRF-09-P-0001-V1_0_0_PSSIG_Cost_Spreadsheet.xls.

sume that the use cases discussed in this document are not specific cases that are optimally addressed by cognitive capabilities, but rather representative of a class of cases that can be *effectively* addressed by cognitive capabilities.

6. Emergency communications in support of incident response are based on guidelines of appropriate multi-agency incident command and coordination, such as the National Incident Management System (NIMS) in the United States, the Gold and Silver coordinating groups in London, and comparable incident command structures elsewhere.

7. Scenarios assume non-cognitive legacy radios will continue to be used, and need to be considered within the solutions provided in the use cases. We assume that any implementation of cognitive radio capabilities will include capability to interoperate with and/or to avoid interference with legacy (non-cognitive) radios.

8. There may be a need to connect public safety radio system devices with non-public safety radios, such as commercial cellular network handsets. Part of the use case analysis addresses the technical capabilities required to ensure that the public safety radios/networks are not compromised by the inclusion of the non-public safety radios.

9. Cognitive radios are part of a broader set of capabilities for maintaining the safety of the public and responding to incidents. Cognitive radios support the communications, which in turn supports the allocation of resources and the command and control necessary to effectively respond to an incident. As a result, in some cases we identify cognitive capabilities that are useful in ensuring that the right information is transmitted at the right time to the right people; in some cases the needed cognitive capability is a combination of the capabilities of the communications system and the cognitive capabilities of associated applications.

3 Methodology

Our methodology used within this document establishes use cases within the context of multiple scenarios based on actual or credible hypothesized events relevant to public safety. We analyze each scenario in detail to determine how cognitive radio capabilities could positively impact communications supporting the public safety activity. The results of each individual scenario analysis were compiled to create a final analysis of the potential application of cognitive radio technology for public safety applications, along with a description of technical, regulatory, and procedural issues that must be considered and addressed prior to realizing the described benefits of enhanced communications capabilities.

In each scenario we analyze the events to derive use cases. This document includes analysis of a hypothetical scenario of a chemical plant explosion. The analysis of each scenario follows a common approach:

- Develop a timeline of events in the scenario. (In this report, we also added architectural framework representations of some aspects of the scenario.)
- Identify points in the timeline in which cognitive capabilities could enhance communications (the cognitive use cases). For each use case, identify how the use case changes the physical, network, procedural, regulatory, and chronological elements of the scenario.
- Analyze the derived use cases in terms of the technical, regulatory, and procedural issues that need to be addressed to achieve the enhanced communications.

The remainder of this section describes this approach in more detail.

3.1 Select Scenarios

The first step in the overall methodology was to identify scenarios for analysis. The scenarios need to be sufficiently rich in activity to support analysis of a broad segment of use cases, with sufficient realism to maintain credibility with the stakeholders (in the case of the public safety community), and sufficient detail to allow derivation of relevant cognitive radio capabilities from the use cases. The scenario selected for Volume 1[8] of this series was the series of bombings that took place in London on July 7, 2005. It was selected based on the credibility of a real scenario and the extensive documentation in after action reports[9]. While that scenario provided an excellent starting point, and highlighted certain areas for cognitive capabilities, it did not reflect the whole breadth of possible use cases. Thus for this volume we chose a hypothetical scenario, although it also incorporates aspects of real-life scenarios.

3.2 Develop Timeline and Architectural Diagrams

The second step in the analysis process was to establish a detailed timeline of scenario events. Since the scenario described in this study is a hypothetical scenario, we used best estimates to establish a

[8] SDR Forum, *Use Cases for Cognitive Applications in Public Safety Communications Systems, Volume 1: Review of the 7 July Bombing of the London Underground*, Document SDRF-07-P-0019-V1.0, 8 November 2007, available at www.wirelessinnovation.org.
[9] Greater London Authority, *Report of the 7 July Review Committee*, June 2006.

timeline of events. We also developed some high level Operational View architecture diagrams to assist in documenting the actors and activities described in the scenario.

3.3 Identify Capability Gaps

Having established the scenario timeline, the next step was to identify those situations in which cognitive capabilities and dynamic spectrum access could have positively impacted the response(s) defined in the scenario. We began by considering what types of communications capabilities generally available today would typically be employed for the specific scenario event. We then considered if there are limitations associated with those current capabilities (e.g., inability to establish a communications channel where information is needed, the time needed to set up a communications link does not meet the needs of the incident response, the communications channel is not sufficiently reliable). We defined these limitations as "gaps" between technological capabilities that are currently available and those that would be ideal for incident response. In determining where there are gaps, we considered the following types of questions to determine whether cognitive radio technology could enhance communications capabilities:

- Are there communications capabilities and links that are needed and do not exist at that point in the scenario?
- Are there communications capabilities and links that are established but need to be established in a timelier manner?
- Are there communications capabilities and links that are established in a timely manner whose performance needs to be improved?

By considering these questions in context of the timeline of scenario events, we identified situations in which cognitive capabilities could enhance communications capabilities. The application of cognitive radio capabilities to resolve these situations defines the scenario cognitive use cases described in this report.

3.4 Analyze Use Case

For each identified use case, the next step was to analyze each use case with respect to:

- How cognitive capabilities would impact the communications of the responders,
- How cognitive capabilities would potentially impact the response scenario, and
- Any potential negative impacts that could occur if the cognitive capability were part of the scenario.

We also recognize that the use cases described in Section 5 require functional capabilities that are not necessarily available using technology currently available. (In fact, one of the purposes of this document is to provide input to a gap analysis to identify technology readiness needs.) As the focus of this document is on functional capabilities rather than available technologies, we deliberately attempted to place as few constraints as possible on technologies that would need to be deployed to realize the use cases. We considered capabilities that were realistic even if they would require future research and development before they could be implemented. The Public Safety SIG's approach was to first lay a foundation of needed capabilities and then allow other researchers to assess the level of technological advancement required to realize the proposed capability.

Likewise, regulatory, policy, and procedural considerations did not constrain the identification of potential use cases. Regulatory and procedural implications and/or required changes were also noted in the analysis section.

When considering the use cases, we identified five aspects of the communications environment that are useful in framing key issues and challenges. Each of these aspects may change over time:

1. **Physical:** This aspect is concerned with the physical world, including issues of geography, geometry, topography, proximity, density, RF propagation characteristics, and locale. What resources are where, and how can they deploy to where they are needed? How large is the area for which communications coverage is required? What is the geometric distribution of injured people, hospitals with capacity available, and transport to move them? How are responders moving during the scenario timeline and how is the geographic layout of the responders changing over time (e.g., expanding a perimeter)?
2. **Network:** This item deals with technical issues associated with how information flows during normal operations, in response to the scenario emergency and the restoration of failed systems. How are radio systems structured, and how do they connect with other networks such as personal area networks, commercial systems such as the telephone network or Wi-Fi/WiMAX capabilities? Is there a need for interoperability? How much bandwidth is needed? What Quality of Service is needed? What kinds of terminals are available? How do all the different agencies talk with each other and distribute data? Does the network use infrastructure, via repeaters, direct peer to peer, or an ad hoc mesh topology? What radio/user authentication mechanisms are used in the network? What cryptographic algorithms support communications security? How are keys distributed? Can radio functionality be modified over the network, or is hands-on intervention needed?
3. **Procedural:** This issue deals with the operational role of people in system management, including authority, command, control, operating procedures, communications security procedures, and activation of contingency plans. Who develops contingency plans? Are there memoranda of understanding (MoU) in place to establish communications interoperability rules and to ensure a chain of command is in place at the time of the incident? Who has command and control of the situation? Who authorizes individuals or groups to operate radios? What is the registration process for new communications devices requiring authentication? Who reviews requests for registration? How are cryptographic keys managed and what are the respective roles of humans and system automation in key management? Who reprograms radios? Who assigns tasks and/or roles to the first responders?
4. **Regulatory:** Regulators administer the use of spectrum by defining use rules/regulations, issuing licenses for radio operation, and resolving issues of interference,. What legal modulation techniques and frequencies can be used? What are the rules for operation in unlicensed spectrum? How can extra spectrum be temporarily made available during emergency conditions? Are frequency-sharing agreements currently in place? What agencies have jurisdiction?
5. **Chronological:** Time is an overarching consideration that applies to each of the other four aspects listed above. During the time before a specific event, there is time for establishing organizations, procuring equipment, recruiting and training personnel, building networks, defining policies and procedures, and development of contingency plans. When an event occurs, the first problem is awareness that something has happened, and then learning

enough to assess the situation. Decisions are then needed to determine the nature of the response, what resources to commit to it, and what actions to pursue. Operations continue until the emergency is resolved and emergency response units involved stand down. After the event is over, an after-action review considers how well the operations were executed, and how lessons learned can be used to improve preparedness for future emergencies. A primary value of cognitive radio capabilities is to support first response users by adapting to a changing RF environment much more effectively than today's non-cognitive systems can.

4 Chemical Plant Explosion Scenario

This is a sequential discussion of events of a hypothetical scenario in which there is an explosion at a chemical plant located in an industrial section of a mid-sized city. Some notes about the scenario:

Events in the scenario are synthesized from multiple sources, including the SAFECOM Statement of Requirements/TR-8 Broadband Task Group scenario, and also after action reports describing a fire at a hazardous materials transfer station in Apex, North Carolina in October, 2006. Specific additional events have been incorporated into this scenario to illustrate specific capabilities of cognitive radio technology.

The setting, Central City, is taken from the FEMA Integrated Emergency Management Course documentation (Document SM100.1, August 1999) Figure 1 provides geospatial reference for the scenario. Two changes to Central City were made for this scenario. First, the size of the chemical plant, which is unspecified in FEMA document, is designated to be approximately the size of the plant in the SAFECCOM Statement of Requirements. Second, a small Army base with a research facility has been added within Central City. In addition, the scenario assumes the following communications networks:

- **Public Safety Land Mobile Radio (LMR):** Central City public safety agencies (EMS, Fire, and Police) use a digital trunked 700 MHz LMR system for voice communications. Talk groups have been established for each first response discipline, plus talk groups are programmed into the system for command use and for interagency interoperability. County, State Police, and other agencies in the region are not authorized subscribers on the Central City system.
- **Chemical Plant Security Voice Network:** The chemical plant has an industrial security and fire suppression team on-site. They normally utilize a UHF radio system for voice communication. A crossband repeater located at the plant is used to patch the plant security radios to a 700 MHz fireground channel for use during emergencies to communicate with first responders.
- **Public/Private 700Mhz Broadband Data Network:** There is a 700 MHz wireless broadband system that has been deployed in the Central City area as part of a public/private partnership, using spectrum shared between public safety and commercial users. The use of network resources is governed by a network sharing agreement that allows greater commercial use of resources during non-emergency situations but network capacity reverts to public safety use, as a priority, during emergency situations. The network is installed along the I-107 corridor, so other public safety agencies do not typically have equipment or public safety access rights to the system.
- **Incident Area Network:** An ad hoc network is established in the immediate area of the chemical plant, operating at 4.9GHz.

The scenario only attempts to capture major events that could impact the communications requirements of the first responders. Numerous other aspects of the scenario are not detailed.

The scenario is presented in two formats. The first format is a narrative sequence of events. The second is a table format in which the sequence of events is organized, along with notes on communications activities and issues, and potential applications of cognitive technology. These potential

applications will form the basis of described use cases. Architectural diagrams are included to assist in depicting the communications needs defined within the scenario.

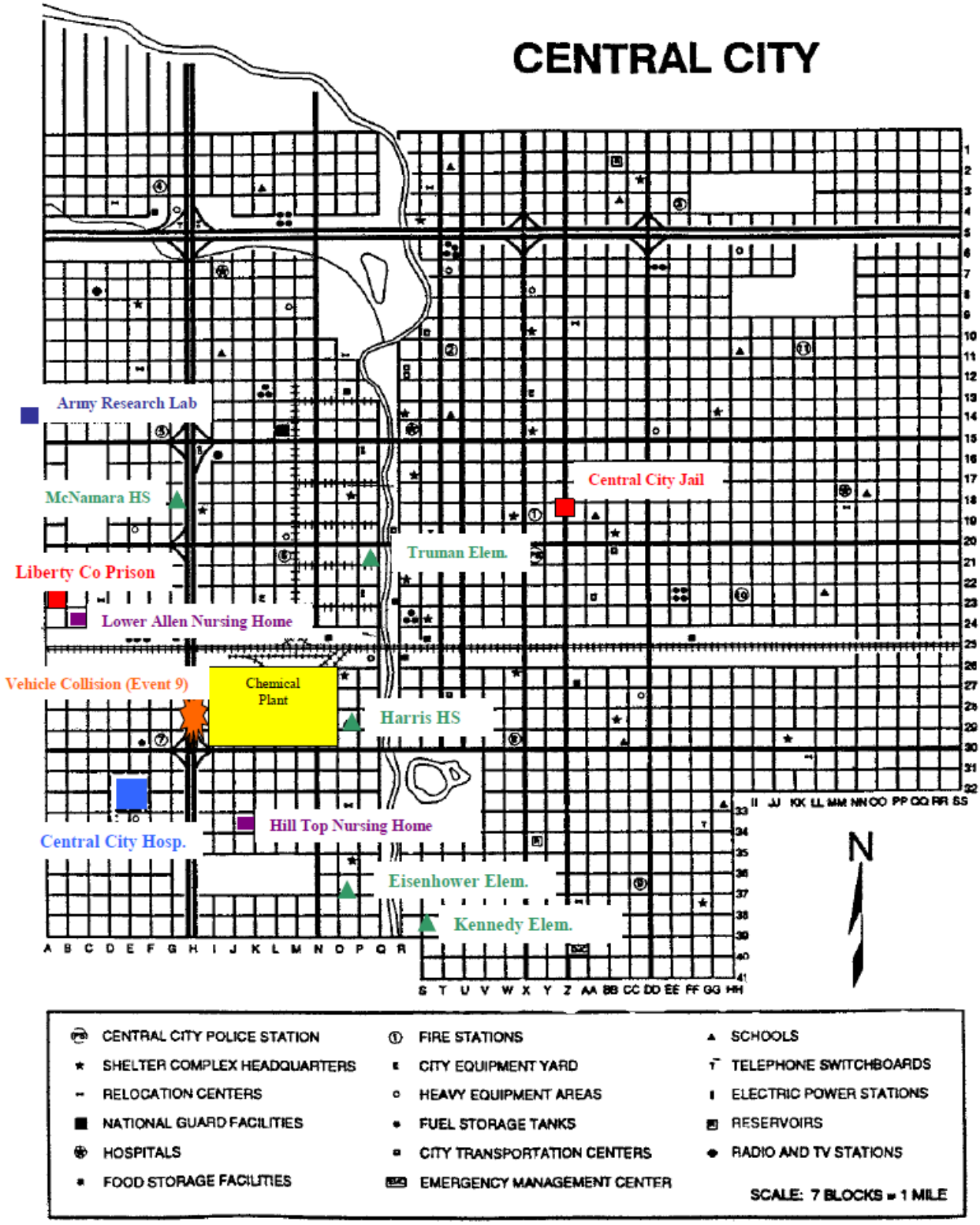

Figure 1: Scenario Map

4.1 Narrative of the Scenario

1. A large explosion occurs, early one afternoon, at a chemical plant in the industrial area of southwestern Central City. The force of the blast shatters windows in several buildings in the plant complex and damages houses in the surrounding area. In the immediate vicinity of the explosion there are a number of casualties, both wounded and deceased. In addition, flying glass injures students within Harris High School, located across the street from the chemical plant. A large fireball is visible, followed by flames. The plant's alarm system automatically alerts 911 Public Safety Answering Point (PSAP) personnel.

2. Fire, Law Enforcement (LE) and Emergency Medical Service (EMS) units are dispatched to the incident; within minutes the 911 PSAP is flooded with calls from motorists and residents. Responders arriving at the immediate vicinity of the explosion establish an Incident Area Network (IAN) for communication.

3. The explosion destroys the cross-band voice repeater used to link the Plant Security Voice Network with the Public Safety LMR system.

4. The Battalion Chief arrives on the scene with the first responding units, assumes incident command, and establishes a Mobile Command Center (MCC) in the back of a command vehicle. The MCC is located at the southwest corner of the plant property. After briefly surveying the area, the Incident Command (IC) team initiates use of their mobile command center and begins to receive information from the Incident Area Network created by the on-site first responder vehicles and personnel.

5. The city Emergency Operations Center (EOC) is activated and communications established with IC personnel at the MCC.

6. Initial responders don Personal Protective Equipment (PPE) then begin to fight the fire and evacuate wounded people that can be reached out of the immediate area.

7. An initial incident perimeter is established. Law enforcement personnel are assigned to perimeter control and to also evacuate Harris High School.

8. A thickening whitish cloud is emanating from the fire scene. Wind direction is from the southeast, spreading the plume north and west of the plant fire. Personnel caught in the cloud without protection begin exhibiting respiratory problems and either evacuate the area or don PPE. Meanwhile (non-Fire) EMS personnel establish triage and command areas outside hot zone/plume area and begin to direct the available resources to identify and handle casualties. The location of the triage/treatment area is disseminated to all first responders on-scene, and area medical facilities are alerted as to the status of the triage/treatment area.

9. The cloud spreads across I-107, adjacent to the plant. Reduced visibility and possibly the effects of the chemicals result in a chain-reaction automobile accident. Additional fire and EMS units are required at this accident scene.

10. IC personnel direct dispatchers to initiate a reverse 911 notification. People in the immediate vicinity of the cloud are directed to take shelter in place; other people are told to evacuate. Police officers assist in notifying and evacuating residents. Additional incident command staff begins to download plant building plans, materials manifests, hazmat databases, weather, plume modeling, etc. – while en route to the scene.

11. The evacuation zone includes the Lower Allen Nursing Home, the Liberty County Prison, and McNamara High School. Mutual response personnel, including Liberty County Sheriff's deputies, Columbia State Police; and police officers from Apple Valley, Deep River, and Fisherville, arrive to assist with the evacuation of nursing home residents. Responders from outside agencies arriving at the incident scene are authenticated into the network.

12. Prisoners are moved from the jail to state prison facilities. National Guard MPs assist in moving the prisoners onto buses.

13. The Law Enforcement (LE) Branch is directed by IC to coordinate with the Department of Transportation (DOT) to configure traffic management assets, such as traffic lights and electronic signs, to divert traffic away from the incident. The accident on I-107 creates a major traffic jam.

14. As the plume spreads, panicky evacuees abandon motor vehicles and flee on foot. Tow trucks are required to clear the streets of abandoned vehicles to facilitate the movement of emergency vehicles

15. Loading on the Public/Private 700 MHz Broadband Data Network reaches the criteria of an emergency as defined in a network sharing agreement. System resources are reallocated so that network capacity is made available for public safety users and reduced for commercial users.

16. A survey of the explosion area is conducted by LE, Fire, and EMS personnel to record geolocation data for casualties, fires, evidence, and the incident perimeter, etc. This information is made available to the IC as an on-line GIS overlay of the explosion area. Network operational information (location and operating parameters of radios, detected signal strength information, spectrum sensing data) is also provided to the COML.

17. As the cloud grows, IC orders the MCC to relocate to a park area several blocks south of the plant. The evacuation area is increased and includes the small Army base located west of town which houses a research facility.

18. Even with the 700 MHz data network resources assigned to public safety, the network slowly reaches capacity. Additional sensors begin transmitting personnel health status information, RFID tags are used for asset management, patient status, etc. Video is used extensively to provide information from inside the cloud to IC.

19. There is significant interference on some of the channels of the Public Safety LMR system. Some firefighters inside the chemical plant itself are having significant difficulty in communicating due to interference.

20. Additional responders are assigned to the event and the geographic scope of the incident continues to increase.

21. Performance of the Public Safety LMR system degrades after a reallocation of frequencies.

22. IC queries the plant manager to attempt to understand what action may have caused the explosion. A temporary network is set up among several police officers and firefighters deployed around the site, equipped with radios and video equipment, and plant engineering staff located at an out of state corporate headquarters. The corporate engineering staff brings up incident video on a computer screen at corporate HQ etc.; HQ engineering staff postulates potential sabotage scenarios that could create the circumstances of this incident.

23. Data from HazMat sensors located on the responder PPE equipment is sent to the EOC for input to the plume model that runs on the computers there. Updated projections of the plume model are then sent to IC staff.

24. Firefighters observe liquid being released in the area of the fire. The Department of Public Works (DPW) is contacted to bring in earthmoving equipment to build a containment berm around the site.

25. Upon further investigation by LE and Fire assets, IC determines that this explosion may not have been an accident; IC directs LE to treat the area as a crime scene and assigns LE detectives to begin an investigation of the crime scene in coordination with Fire Investigators. The Explosive Ordinance Disposal (EOD) team arrives and initiates a secondary explosive device search using remotely controlled robotic devices. When finished, the Unit Commander of the EOD team notifies the LE Branch of IC that no secondary explosive devices have been found.

26. The EMS Branch continues to coordinate the efforts of EMS assets. As casualty information, collected via the RFID tags used by personnel in the field, is displayed onto the command screen the most critical cases are selected for transport to the nearest available hospitals. The EMS Branch believes that the on-scene casualties will overburden the medical facilities selected to handle them. The transportation officer is directed to query the local medical facilities as to their status, and their capacity to accept casualties and what types of casualties can be received. Casualty statistics are available on demand by IC and the EM. In addition, the local medical centers coordinate through the city EOC regarding resource availability.

27. Industrial firefighters and environmental health consultants arrive from outside the region, via police escort. These units do not have standing mutual aid agreements in place with the Central City agencies.

28. A fast moving weather system shifts the wind and plume direction. A new evacuation zone is identified, requiring evacuation of the Hill Top Nursing Home. The MCC is also relocated.

29. Over time the incident is gradually brought under control. All casualties are transported to medical facilities; and the fire at the plant is brought under control.

30. The IC is notified that all of the fires have been eliminated, the hazardous chemical spill has been contained, all of the casualties have been evacuated to appropriate medical facilities, evacuated residents are allowed re-entry, and that the coroner has been directed to begin removal of corpses.

31. First responders who are no longer needed for the incident response are released (and return to home jurisdictions if appropriate).

32. As part of the after action analysis of the incident response by Central City personnel, a detailed analysis of the communications is required.

4.2 Timeline of Events

Event	Communication Activity with Current Capabilities	Gap	Potential Cognitive Capability
1. A large explosion occurs, early one afternoon, at a chemical plant in the industrial area of southwestern Central City. The force of the blast shatters windows in several buildings in the plant complex and damages houses in the surrounding area. In the immediate vicinity of the explosion there are a number of casualties, both wounded and deceased. In addition, flying glass injures students within Harris High School, located across the street from the chemical plant. A large fireball is visible, followed by flames. The plant's alarm system automatically alerts 911 Public Safety Answering Point (PSAP) personnel.	Communications are occurring between dispatch and the fire units and police units over the trunked radio system. Existing land mobile radio (LMR) system accommodates all traffic.		

Event	Communication Activity with Current Capabilities	Gap	Potential Cognitive Capability
2. Fire, Law Enforcement and Emergency Medical Service (EMS) units are dispatched to the incident; within minutes the 911 PSAP is flooded with calls from motorists and residents. Responders arriving at the immediate vicinity of the explosion establish an Incident Area Network (IAN) for communication.	Communication continues among dispatch and the first responders. 911 calls are coming into the PSAP from landlines and cell phones. 911 calls overwhelm the system, exceeding system capacity. Existing land mobile radio (LMR) system accommodates all voice communications traffic among first responders and dispatch.		
3. The explosion destroys the cross-band voice repeater used to link the Plant Security Voice Network with the Public Safety LMR system.	Plant personnel are initially unable to communicate with the first responders due to the damage to the cross connect voice repeater that was intended to provide connectivity between plant security and first responders. A preconfigured tactical crossband repeater is deployed. Existing equipment meets need.		
4. The Battalion Chief arrives on the scene with the first responding units, assumes incident command, and establishes a Mobile Command Center (MCC) in the back of a command vehicle. The MCC is located at the southwest corner of the plant property. After briefly surveying the area, the IC team initiates use of their mobile command center and begins to receive information from the Incident Area Network created by the on-site first responder vehicles and personnel.	On site communications continues among first responders. On-site tactical channels are assigned for voice communications. An Incident Area Network (IAN) among first responders is established to relay information such as location data, biometric monitoring, and so on. Existing equipment meets need.		

Event	Communication Activity with Current Capabilities	Gap	Potential Cognitive Capability
5. The city Emergency Operations Center is activated and communications established with IC personnel at the MCC.	Voice and data communications are required between IC and the off-site EOC. Voice communications uses the Central City Public Safety LMR system, and data uses the shared Broadband Network.		
6. Initial responders don PPE then begin to fight the fire and evacuate wounded people that can be reached, out of the immediate area.	First responders continue communications using LMR equipment and data from sensors integrated into the PPEs (biometric data, hazard detection data etc.).	With current equipment, sensors do not cooperatively use spectrum efficiently. When a large number of sensors are deployed in a small area, contention for spectrum leads to information being delayed, dropped, or blocked, and the number of sensors that can be deployed in the area is limited.	Responders wearing the PPE have wireless sensors that form an ad hoc network using unused spectrum (listen before talk) with cognitive technology. They report the sensor readings back to the MCC which is monitoring the environment in which the first responders are working. Sensors automatically activate and deactivate when equipment is donned or removed or manually. Data rate is adjusted as a degree of threat; threat can be defined in terms of data itself (if no nuclear detection, send less frequently unless detections start); location based (closer to hot spot, more frequent), etc.
7. An initial incident perimeter is established. Law enforcement personnel are assigned to perimeter control and to also evacuate Harris High School.	Police personnel need to communicate for traffic control and evacuation. Channels/talk groups are assigned on the LMR system for perimeter control coordination and evacuation. Police use in-place LMR equipment and channels.		

Event	Communication Activity with Current Capabilities	Gap	Potential Cognitive Capability
8. A thickening whitish cloud is emanating from the fire scene. Wind direction is from the southeast, spreading the plume north and west of the plant fire. Personnel caught in the cloud without protection begin exhibiting respiratory problems and either evacuate the area or don PPE. Meanwhile (non-Fire) EMS personnel establish triage and command areas outside hot zone/plume area and begin to direct the available resources to identify and handle casualties. The location of the triage/treatment area is disseminated to all first responders on-scene, and area medical facilities are alerted as to the status of the triage/treatment area.	The Incident Command Structure (ICS) is structured based in part on available communications capabilities. Talk groups and channel assignments are made based on the availability of communications resources. Personnel are assigned within the ICS based in part of communications capabilities.		
9. The cloud spreads across I-107, adjacent to the plant. Reduced visibility and possibly the effects of the chemicals result in a chain-reaction automobile accident. Additional fire and EMS units are required at this accident scene.	Responders at the accident scene require tactical voice communications among themselves while responding to the accident. Voice communication is also required with IC personnel to coordinate evacuation routes, utilize the triage area, etc… However, these additional communications needs increase bandwidth requirements in the immediate area of the incident. All responders are utilizing the existing LMR for voice communications and the shared broadband network for data communications.		

Event	Communication Activity with Current Capabilities	Gap	Potential Cognitive Capability
10. IC personnel direct dispatchers to initiate a reverse 911 notification. People in the immediate vicinity of the cloud are directed to take shelter in place; other people are told to evacuate. Police officers assist in notifying and evacuating residents. Additional incident command staff begins to download plant building plans, materials manifests, hazmat databases, weather, plume modeling, etc. – while en route to the scene.	Police officers require communications to coordinate evacuation efforts and perimeter control activities. IC requires broadband data capabilities to download information. Existing LMR and broadband network used.		
11. The evacuation zone includes the Lower Allen Nursing Home, the Liberty County Prison, and McNamara High School. Mutual response personnel, including Liberty County Sheriff's deputies, Columbia State Police; and police officers from Apple Valley, Deep River, and Fisherville, arrive to assist with the evacuation of nursing home residents. Responders from outside agencies arriving at the incident scene are authenticated into the network.	Outside agency responders who are not subscribers to the Central City Public Safety LMR cannot immediately communicate to other incident responders. Currently deployed technology requires a network gateway, radio cache, or shared channel (including air interface). Communications is required between arriving first responders and the local network infrastructure to verify that the responders have the appropriate credentials to be allowed access to the network. Appropriate authentication protocols are used.	Gateways tie up multiple frequencies/ channels for a single "conversation", are spectrally inefficient, and only work if the users are within the coverage area of the systems or radios being linked. Caches require ongoing maintenance and are a resource that is otherwise underutilized. Shared channels are only viable in specific situations	Voice radios of responding agencies are not compatible; radios are reprogrammed over the air as needed once users are authenticated into the system.

Event	Communication Activity with Current Capabilities	Gap	Potential Cognitive Capability
12. Prisoners are moved from the jail to state prison facilities. National Guard MPs assist in moving the prisoners onto buses.	Outside agencies do not have channels for communication. The radio system for the jail only provides coverage in the immediate vicinity of the jail. Normal transport channels are unavailable. School buses which are being used to move prisoners only have legacy voice radio equipment programmed to the school bus system frequencies.	Normal transport channels are unavailable, Jail radio system does not provide coverage beyond the jail grounds. School bus radios are not reconfigurable	Radios carried by jail and national guard personnel are reprogrammed to include a free interoperability channel, the State Prison System Transport channel, as well as the ICS assigned channel for emergencies.
13. The LE Branch is directed by IC to coordinate with the Department of Transportation (DOT) to configure traffic management assets, such as traffic lights and electronic signs, to divert traffic away from the incident. The accident on I-107 creates a major traffic jam.	Data is transmitted to control traffic signals and update variable message signs. Data is also transmitted to in-car navigation systems.(e.g., updates to the status of evacuation routes, location of the hazardous plume)	Methods for rapidly communicating location specific information to first responders as well as civilians are limited.	Cognitive capabilities also reconfigure the network to support coordination with in-vehicle navigation systems (first responders & civilians).
14. As the plume spreads, panicky evacuees abandon motor vehicles and flee on foot. Tow trucks are required to clear the streets of abandoned vehicles to facilitate the movement of emergency vehicles	A voice gateway must be set up to allow law enforcement, Dept of Transportation, and tow truck operators to communicate.	The tow truck operators have legacy equipment (e.g., two-way or Citizens Band radio) that cannot be reconfigured, and do not share channels with public safety networks. Manual set up of the necessary gateway patch requires time and specialized expertise.	Since tow truck operators do not have advanced reconfigurable radios, the public safety network automatically configures a gateway patch to link IC staff with DoT and tow truck operators as needed.

Event	Communication Activity with Current Capabilities	Gap	Potential Cognitive Capability
15. Loading on the Public/Private 700Mhz Broadband Data Network reaches the criteria of an emergency as defined in a network sharing agreement. System resources are reallocated so that network capacity is made available for public safety users and reduced for commercial users.	Broadband data communications requirements exceed network capacity required for routine public safety operations.	With current technology, data is delayed or transmissions are blocked/dropped. Any attempt to manage use of the spectrum is manual. No additional capabilities can be accessed.	Network automatically (using cognitive capabilities) identifies emergency criteria, and reallocates spectrum from commercial to public safety use as per a network sharing agreement. Additional channels/capacity is automatically allocated in real-time, based on ongoing bandwidth requirements. Availability of additional network capabilities such as satellite broadband services are also assessed, and data is routed as needed using additional capabilities.
16. A survey of explosion area is conducted by LE, Fire, and EMS personnel to record geolocation data for casualties, fires, evidence, and the incident perimeter, etc. This information is made available to the IC as an on-line GIS overlay of the explosion area. Network operational information (location and operating parameters of radios, detected signal strength information, spectrum sensing data) is also provided to the COML.	The Incident Commander and Comm Unit Leader require information on the RF environment and the location of communications assets to most efficiently management the communications resources.	Information regarding the RF environment and location of communications assets is not available for network operations management	RF and geolocation information is transmitted to the Comm Unit Leader. The Comm Unit Leader uses the information for network management (power output, talk group assignment, frequency reuse).
17. As the cloud grows, IC orders the MCC to relocate to a park area several blocks south of the plant. The evacuation area is increased and includes the small Army base located west of town which houses a research facility.	Voice channels/talkgroups established via the LMR system for communication between Army and IC.	Current technology requires a gateway, cache, or shared channel which are limited (see Event 11).	Voice radios of responding agencies are not programmed correctly for the incident; radios are reprogrammed over the air as needed.

Event	Communication Activity with Current Capabilities	Gap	Potential Cognitive Capability
18. Even with the 700MHz data network resources assigned to public safety, the network slowly reaches capacity. Additional sensors begin transmitting personnel health status information, RFID tags are used for asset management, patient status, etc. Video is used extensively to provide information from inside the cloud to IC.	The increasing data transmissions overwhelm the available communications capabilities.	With current technology, data is delayed or transmissions are blocked/dropped. Any attempt to manage use of the spectrum is manual. No additional capabilities can be accessed. (See Event 13.)	Cognitive capabilities support QoS/bandwidth management; some functionality can be incorporated into policy. Vital sign monitoring data refresh rate is reduced, and frame rate reduction is applied to some video providing back to IC from inside the cloud.
19. There is significant interference on some of the channels of the Public Safety LMR system. Some firefighters inside the chemical plant itself are having significant difficulty in communicating due to interference.	Voice transmissions must frequently be repeated.	The only recourse is to manually determine whether there is a different frequency/ channel available for use (which requires the frequency to already be programmed into each user's radio, or hands-on manual reprogramming.)	Cognitive based interference mitigation techniques reduce the interference on the channel. In some cases the level of interference cannot be managed, and the COML is alerted to the problem and alternatives that can be implemented. In some cases, radios are reconfigured over the air to utilize new channels.
20. Additional responders are assigned to the event and the geographic scope of the incident continues to increase.	The trunked voice radio system begins to reach capacity, and there are few other channels that can be utilized for incident command. 700 MHz national interop channels are assigned for use in this incident and made unavailable for other uses in the region. Despite these steps, capacity limits are again reached. A spectrum mutual aid agreement is exercised that allows frequencies that are normally licensed to Metropolis Police Department to be used by the IC.	Without the ability to perform real-time adjustments to the system, increasing numbers of calls are queued. Exploiting the additional frequencies with current technology is extremely difficult as each radio would need to be reprogrammed manually.	Policy definitions are incorporated into the cognitive capabilities that determine the allocation of frequencies. Monitoring devices monitor capacity and reassign channels/frequencies as needed. Non-mission critical communications is reassigned to unlicensed frequencies (perhaps TV white space). Cognitive capabilities support over the air reconfiguration of radios.
21. Performance of the Public Safety LMR system degrades after a reallocation of frequencies.	The performance of the voice network degrades as a result of changes made in previous events.	With current technology performance issues must be addressed manually.	Cognitive capabilities include a "rollback" provision that allows changes to be retracted to a previously defined state.

Event	Communication Activity with Current Capabilities	Gap	Potential Cognitive Capability
22. IC queries the plant manager to attempt to understand what action may have caused the explosion. A temporary network is set up among several police officers and firefighters deployed around the site, equipped with radios and video equipment, and plant engineering staff located at an out of state corporate headquarters. The corporate engineering staff brings up incident video on a computer screen at corporate HQ etc.; HQ engineering staff postulates potential sabotage scenarios that could create the circumstances of this incident.	Video and other data communicated from sensors through Incident Area Network out to Wide Area Network. Currently available gateways can be used to create the necessary inter-network connections.	Tools for management of data flow between disparate networks, particularly if the data rates and capacities of the networks are significantly different, are limited.	Cognitive-based bandwidth management may be applied to manage data flow on each network and between networks.
23. Data from HazMat sensors located on the responder PPE equipment is sent to the EOC for input to the plume model that runs on the computers there. Updated projections of the plume model are then sent to IC staff.	Monitoring data is transmitted to the EOC; modeling data back to IC. Existing links are used to transmit the data.	Current tools for bandwidth management are limited.	Cognitive capabilities are used to optimize backhaul (can include satellite communications) Cognitive capabilities of the sensors are used to identify appropriate frequencies for communication.
24. Firefighters observe liquid being released in the area of the fire. DPW is contacted to bring in earthmoving equipment to build a containment berm around the site.	Voice channels/talk groups are established on the trunked radio system for communication among IC and DPW. Current technology for channels/talk groups is adequate.		

Event	Communication Activity with Current Capabilities	Gap	Potential Cognitive Capability
25. Upon further investigation by LE and Fire assets, IC determines that this explosion may not have been an accident; IC directs LE to treat the area as a crime scene and assigns LE detectives to begin an investigation of the crime scene in coordination with Fire Investigators. The EOD team arrives and initiates a secondary explosive device search using remotely controlled robotic devices. When finished, the Unit Commander of the EOD team notifies the LE Branch of IC that no secondary explosive devices have been found.	Trunked voice channels/talk groups are established for voice communication among IC and EOD, IC and investigators. Data is transmitted, between robots and control, via the broadband network.		

Event	Communication Activity with Current Capabilities	Gap	Potential Cognitive Capability
26. The EMS Branch continues to coordinate the efforts of EMS assets. As casualty information, collected via the RFID tags used by personnel in the field, is displayed onto the command screen the most critical cases are selected for transport to the nearest available hospitals. The EMS Branch believes that the on-scene casualties will overburden the medical facilities selected to handle them. The transportation officer is directed to query the local medical facilities as to their status, and their capacity to accept casualties and what types of casualties can be received. Casualty statistics are available on demand by IC and the EM. In addition, the local medical centers coordinate through the city EOC regarding resource availability.	Medical data is transmitted, via the shared broadband network, from patients to medical personnel, ambulances, and hospitals, The increasing amount of data saturates existing channels.	There are no tools to provide real-time bandwidth management allowing EMS personnel to prioritize the most important transmissions.	Cognitive capabilities support QoS/bandwidth management as broadband data requirements increase. Patient status is used to prioritize life critical transmissions over data relating to less critical patients.
27. Industrial firefighters and environmental health consultants arrive from outside the region, via police escort. These units do not have standing mutual aid agreements in place with the Central City agencies.	Channels/talk groups are established to support communications among IC and assisting non-first responder agencies.	Current technology is limited; for example, a gateway or pre-planned patch may be used (see Event 11 for description of limitations.) Without pre-planning there are limited capabilities to link to non-first responders.	Cognitive capabilities are used to configure the network to establish a channel to interoperate with non-first responders (without disrupting mission critical communications). This allows direct communications as needed for interface with industrial firefighters, public transportation buses for evacuations, etc.

Event	Communication Activity with Current Capabilities	Gap	Potential Cognitive Capability
28. A fast moving weather system shifts the wind and plume direction. A new evacuation zone is identified, requiring evacuation of the Hill Top Nursing Home. The MCC is also relocated.	As communication vans, tactical broadband repeaters, and personnel move about Rayleigh fading occurs. Signal degradation disrupts network communications.	Tools to maintain network connectivity and optimum performance while key nodes are being relocated are limited.	
29. Over time the incident is gradually brought under control. All casualties are transported to medical facilities; and the fire at the plant is brought under control.	At various points in the incident response, completion of tasks result in the release or reassignment of response teams to/from the incident, and release or reassignment of the communications resources that were required to support their activities.	Currently, any changes to radios in support the incident response must be reversed manually. Also note that any of the changes noted in the Potential Cognitive Capabilities must also be able to be reversed.	Cognitive radio capabilities and over the air reconfiguration are used to release communications resources (including frequencies) that are no longer needed and restore radios to pre-incident status for responders who are returning to home agencies.
30. The IC is notified that all of the fires have been eliminated, the hazardous chemical spill has been contained, all of the casualties have been evacuated to appropriate medical facilities, evacuated residents are allowed reentry, and that the coroner has been directed to begin removal of corpses.	As various elements of the incident response are dismissed, communications assets need to be reconfigured accordingly; either to vacate reallocated resources or to release network capacity that had been commandeered, via shared network capacity agreements, specifically to support the incident response.	Current technology requires mostly manual reconfiguration.	Cognitive capabilities can facilitate restoring communications as the incident ramps down.
31. First responders who are no longer needed for the incident response are released (and return to home jurisdictions if appropriate).	As an extension of the previous event, as the incident ends the communications resources must be returned to their pre-incident state.	Current technology requires mostly manual reconfiguration.	Cognitive capabilities facilitate restoring radios to pre-incident status.
32. As part of the after action analysis of the incident response by Central City personnel, a detailed analysis of the communications is required.			Part of the cognitive capability should include audit and logging information for post incident analysis. Information could include cognitive-based decisions, communications events, actions taken, etc.

4.3 Architecture Representation

An architecture description is a representation of a defined domain, as of a current or future point in time, in terms of its constituent parts, what those parts do, how the parts relate to each other and to the environment, and the rules and constraints governing them. An architecture description is composed of architecture products that are interrelated within each view and also interrelated across views. Architecture products are those graphical, textual, and tabular items developed in the course of gathering architecture data, identifying their composition into related architecture components or composites, and modeling the relationships among those composites to describe characteristics pertinent to the architecture's intended use.

A full set of architectural products include:

- Operational Views (e.g., OV-1, 2, 3, etc.) that describe the tasks and activities, operational elements and nodes, and information exchanges required to accomplish a task or mission.
- System Views (e.g., SV-1,2,3, etc.) are a set of graphical and textual products that describes systems and interconnections providing for, or supporting system functions required by the user(s) to accomplish his/her task or mission.
- Technical Views (e.g., TV-1, 2…9) are the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements.
- All Views (e.g., AV-1, 2) provide information pertinent to the entire architecture but do not represent a distinct view of the architecture.

To help illustrate these points, at a high level, the wireless communication need lines, user/participant organization and nodal representation of the combined events articulated in the scenario, we have included three Operational Views. Note that these views are specific to the activities represented in the scenario outlined in Section 4.1, and are not intended to be a complete set of the activities that would occur in a real scenario. As an example, for simplification purposes, we have not included the logistics element of the incident response.[10]

The **OV-1** (see Figure 2) is a high-level operational concept graphic that describes a mission or capability (e.g., fight a fire) and highlights main operational nodes (where human activities take place) and interesting or unique aspects of operations. It provides a description of interactions between the subject architecture and its environment and between the architecture and external systems. A textual description accompanying the graphic is crucial as graphics alone are not sufficient for capturing the necessary architecture data. The textual description, in our case, is the Chemical Plant Explosion Scenario document.

[10] The Wireless Innovation Forum is undertaking a project, Information Processing Architecture (IPA) that will use these architectural tools to aid in defining, designing and selecting Cognitive Radio processes relevant and useful to Communication System stakeholders. The project will, via a top-down approach, facilitate an improved understanding of the structure and relationships between Information Systems that span user domains, and allow users to assess the role of their systems with these architectural products.

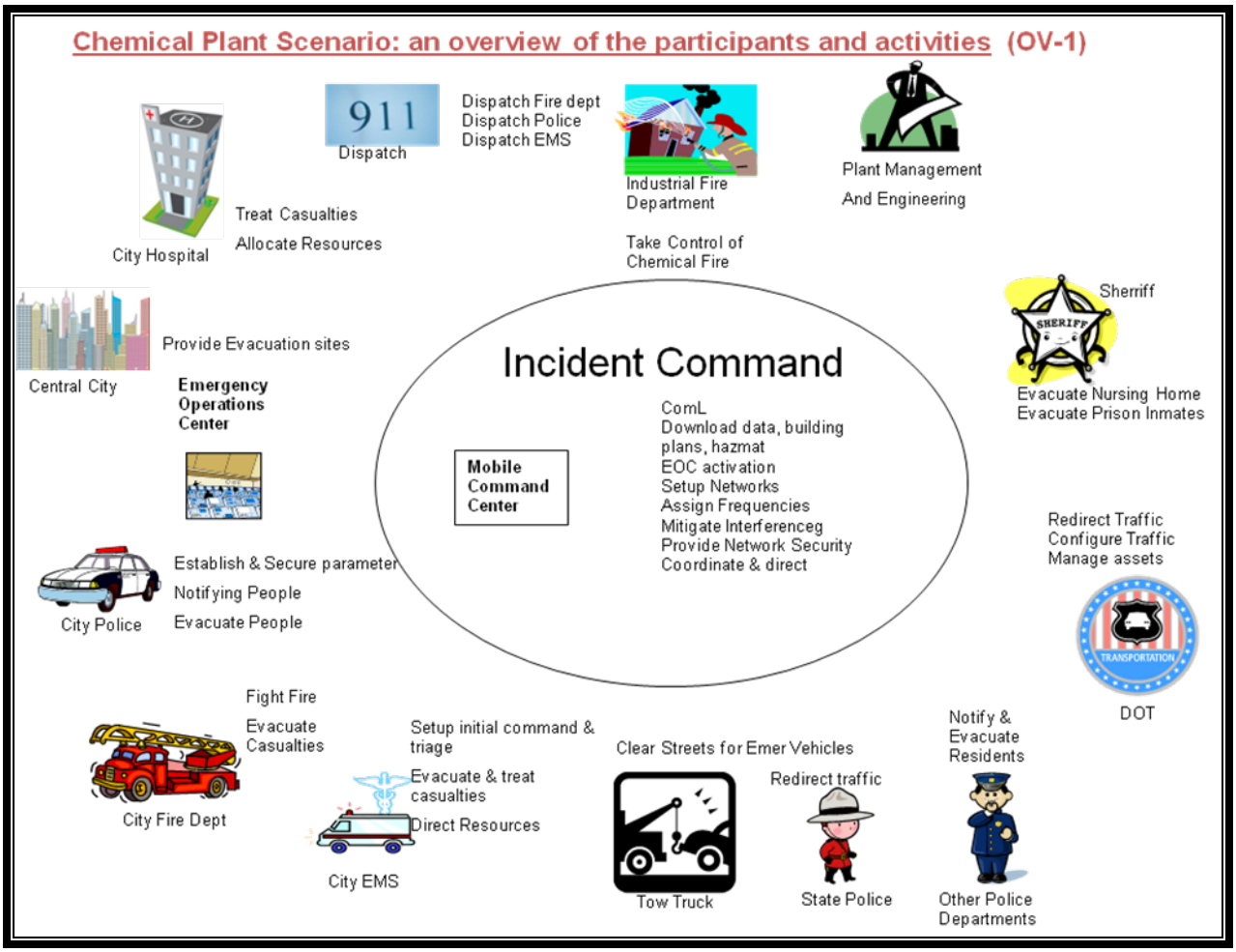

Figure 2: OV-1 Architecture Diagram

The **OV-2** (see Figure 3) is the operational node connectivity description that graphically depicts the operational nodes (or organizations) with need lines between those nodes that indicate a need to exchange information. The graphic includes internal operational nodes (internal to the architecture) as well as external nodes. An OV-2 is intended to track the need to exchange information from specific operational nodes (that play a key role in the architecture) to others. OV-2 does not depict the connectivity between the nodes.

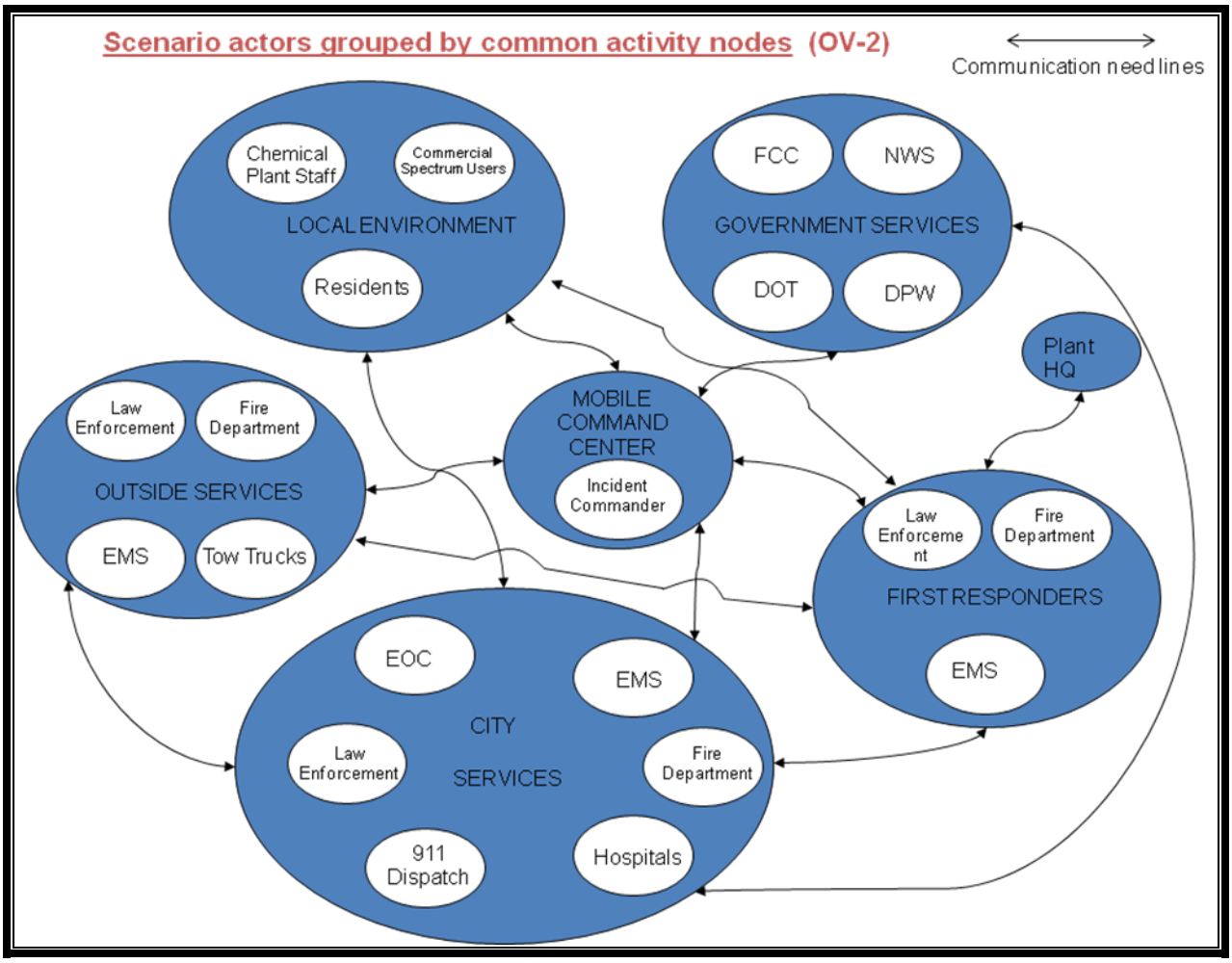

Figure 3: OV-2 Architecture Diagram

The **OV-4** (see Figure 4) is an organizational relationships chart that illustrates the command structure or relationships (as opposed to relationships with respect to a business process flow) among human roles, organizations, or organization types that are the key players in an architecture. It clarifies the various relationships that can exist between organizations and sub-organizations within the architecture and between internal and external organizations. Organizational relationships are important to depict in an OV (for a current architecture), because they can illustrate fundamental human roles (e.g., who or what type of skill is needed to conduct operational activities) as well as management relationships (e.g., command structure or relationship to other key players). Also, organizational relationships may influence how the operational nodes in an OV-2 are connected.

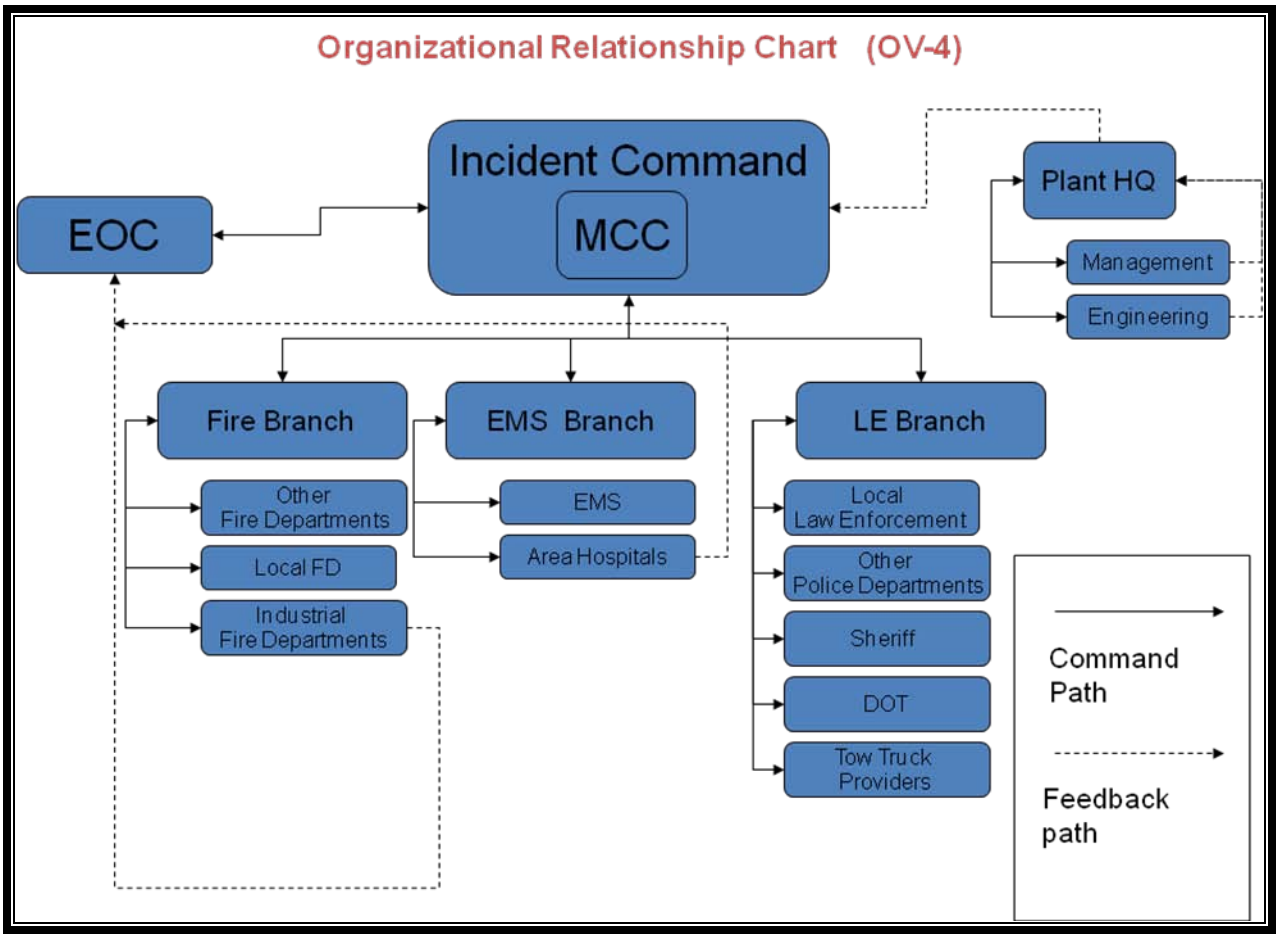

Figure 4: OV-4 Architecture Diagram

5 Use Cases

A number of potential cognitive use cases have been identified based on the scenario timeline as described in the preceding section. In this section, each use case is discussed in much greater detail. The use cases are ordered in descending priority based on operational relevance and feasibility as provided by the public safety practitioners who provided input to and feedback on the report.

Table 1: Use Cases by Event

Event	Use Case	Priority
6	8: Cognitive sensor network	Medium
11	1: Role-based radio reconfiguration	High
12	1: Role-based radio reconfiguration	High
13	5: Reconfigurable repeater/gateway 6: Interface with non-first responders	High Medium
14	5: Reconfigurable repeater/gateway 6: Interface with non-first responders	High Medium
15	3: Resource management in a shared public/private network	Medium
16	2: Resource management in a dedicated public safety network	High
17	1: Role-based radio reconfiguration	High
18	4: Coverage performance improvement	Medium
19	4: Coverage performance improvement	Medium
20	1: Role-based radio reconfiguration 2: Resource management in a dedicated public safety network	High High
21	7: Revert to previous state	Medium
22	2: Resource management in a dedicated public safety network	High
23	2: Resource management in a dedicated public safety network	High
26	2: Resource management in a dedicated public safety network	High
27	5: Reconfigurable repeater/gateway 6: Interface with non-first responders	High Medium
29	7: Revert to previous state	Med
30	7: Revert to previous state	Med
31	7: Revert to previous state	Med

5.1 Use Case 1: Role-Based Reconfiguration

There are a number of events in the scenario in which the first responders from multiple agencies are arriving to support the incident response. Given the scope of the incident, these responders are not from jurisdictions within which the incident is occurring, but are from outside areas for which there are no standing mutual aid agreements and pre-planned communications interoperability capabilities. This means that upon arrival to the incident their radios are not interoperable with local communications systems in use for incident response. The concept of this use case is that arriving radios can be reconfigured specifically to facilitate capabilities that the responder requires, based on the arriving responders role within the incident response structure.

The capability that the arriving radio should provide is a function of the role that the responder user is performing—for example, supervisors in the incident command structure may need more capabilities than other users. This approach provides greater control of communications resources and ensures that interoperability does not result in "everyone talking to everyone." Once a radio is reconfigured, test messages should be sent to ensure that the reconfiguration was successfully executed.

As with any of the use cases that involve reconfiguration of the radio, it is also necessary to be able to rollback reconfigurations to a previous state, and to the pre-incident state on incident completion. This rollback capability is addressed as a separate use case (see Section 5.7).

The impact of this use case can be greatly enhanced by the use of over-the-air reconfiguration/reprogramming. In the described scenario, an assumption is made that arriving radios can be reconfigured while responders are either en route to the incident, or in the field, as needed as responders are reassigned. However, the use case for role-based reprogramming can also be applied even without over-the-air reconfiguration; in this case cognitive capabilities can still provide reconfiguration information even thought the radios must be physically connected to a computer (i.e., "tethered") to be reconfigured. Thus for the discussion in Section 5.1, we focus on the use case to link radio configuration to the roles of a first responders, and make no assumptions about the process by which the radio is reconfigured—specifically, this use case could be realized using current methods of reprogramming the radio by physical connection to computer.

5.1.1 Summary of Scenario Situation

In terms of the aspects of the public safety communications environment:

1. **Physical:** There are numerous first responders who are arriving to support the incident response. They either report to a staging area, or (in conjunction with Use Case 2) register with incident command while enroute to the incident. They are then physically relocated within the RF coverage footprint of the network(s) supporting incident response communications.
2. **Network**: The first responders have radios which are not pre-configured to interoperate with the network(s) supporting incident response communications, or limited access to nationwide interoperability frequencies. Thus, initially, they have no radio connectivity with the incident response team.
3. **Procedural**: There are several possible procedures based on the technology used to provide interoperability. If cache radios are handed out, there are procedures defining the use and responsibility for the cache radios. If some type of gateway is used to patch channels/frequencies of the arriving first responders and the existing network, there are procedures defining authorization of use of the patch as well as responsibilities and use of the channels/frequencies. There are also defined procedures that define roles and responsibilities of an incident command structure. (In the United States, for example, the procedures are defined as part of the National Incident Management System, or NIMS.)
4. **Regulatory**: All channels/frequencies used are licensed public safety frequencies. Therefore there are no regulatory implications of this use case.
5. **Chronological:** Either a patch or gateway device must be activated to bridge frequencies, a task taking anywhere from a few minutes to an hour or more (see Use Case 3 for a more

detailed discussion of gateway capabilities). Reprogramming a radio to operate on the network(s) supporting incident response communications can take as little as take a few minutes (assuming permissions are in place).

5.1.2 Capability Shortfall

Current systems provide limited and static capability to configure radios based on the roles and responsibilities of the radio user. Some agencies have "supervisor" radios which are configured to provide different capabilities than radios given to other personnel, but these capabilities are often built into the radio and cannot be changed. Some radios can also be reconfigured to include needed channel/frequency assignments and functions, but this is a manual process. In addition, such program templates are typically predefined and not modified during the course of an incident.

As a result, responders generally have identical capabilities in their radios. In the event of a major incident, in which responders arrive from outside the jurisdiction where the incident is occurring, incompatible arriving radios need to be reprogrammed to support the incident response. Because of the general static nature of radio configuration templates and the "one-size-fits-all" approach, responders' radios are programmed generically. The challenge is that either a very limited number of functions and channels are provided, which may limit the responders' capabilities, or the maximum capability is provided, an option which opens the door for the chaos of "everyone talking to everyone."

Note that this use case assumes that radio interoperability is achieved by reconfiguring the arriving responders' radios to operate within the local network(s) supporting incident response communications, as opposed to configuring the network (by activating a patch or gateway capability).

While most of the above discussion is based on providing capabilities to users based on their role, this use case also includes managing capabilities for all network users based on emergency status, responder role, and optimizing use of network-wide resources. For example, an issue recently observed on regionally trunked radio systems, is unintended consequences of public safety personnel/responders who are not actively involved in a response remotely monitoring response activities via the trunked system talk-groups. For example: an off-duty responder monitoring over the network from a location (home) that is a significant distance from the incident site (using network capacity to transport the incident communications (audio) to a remotely connected location away from the incident). This activity may be well-intentioned and often legitimate from the perspective of first responders who are rotated in and out of the incident and want to maintain situational awareness before returning to the incident. This may also occur from the perspective of lending agency dispatch centers who want to monitor activities of mutual assistance activities to which local resources are deployed. This can impact local radio system resource availability on network segments that may be capacity limited, invisibly consuming local over the air resources needed to ensure continuity of local services outside the area and unrelated to the monitored incident. (For instance, during the recent bridge collapse in Minnesota, network resources on the city system met the needs of incident responders, but network segments on the periphery of the regional system were capacity limited. Remotely monitoring the incident impacted the ability to dispatch ongoing non-incident related calls.) Reconfiguring user radios and prioritizing the network resources appropriately can ensure that the communications channels are used for the highest priority needs, for both the incident as well as ensuring resource availability required for continuity of ongoing operations away from the incident.

5.1.3 Description of Use Case

The concept of this use case is to use cognitive capabilities to create the appropriate radio programming template for the radio, based on the radio user's role within the incident response. In addition, this capability would be dynamic so that as the responder's role changes, the radio is reprogrammed/reconfigured to provide the necessary supporting capabilities.

With respect to the specific aspects of the scenario situation noted in Section 5.1.1, this use case would result in the following:

1. **Physical:** There is no change in the physical deployment of assets.
2. **Network**: Reconfiguration of the radios provides role-based connectivity to the network(s) supporting incident response communications.
3. **Procedural**: The primary procedural change in this use case is explicit definition of responder roles in an incident, and explicit definition of the communications capabilities and operating procedures associated with those roles. (Note that definition of roles and communications capabilities must be done as part of pre-incident planning.)
4. **Regulatory**: All channels/frequencies to be used are licensed public safety frequencies. Therefore there are no regulatory implications of this use case.
5. **Chronological:** This use case does materially change the timelines involved in reconfiguring radios for responders' use in an incident. Radios that are not operable with the network(s) supporting incident response communications must be reprogrammed.

5.1.3.1 Functional Capabilities

Cognitive radio functions required to realize this use case include the following:

- Explicit definition of user roles within an incident response structure. The appropriate (based on the incident command procedures in place for the jurisdiction or region) framework for identifying responder roles should be used as a baseline. One of the technical challenges is the cognitive system's ability to react to the adaptations and tailoring of an overall framework that is required to meet the user requirements within a specific incident.
    - User roles could be organized in a hierarchical (or other) structure. For example, roles could be defined for fire, law enforcement, medical, etc. Then within each of these categories there could be appropriate subcategories, (e.g. EMT, doctor) and ending with a specific role such as on-site triage.
- Electronic storage of a user's credentials (e.g., an RFID chip). Credentials could contain digital certificates and a listing of all roles that the individual is qualified to fulfill within an incident response. Such a function would allow the user to authenticate his credentials using any radio capable of querying the network, and to inform the network of their presence and qualified roles. Command authorities could then make an informed decision as to how the individual could best function in support of the incident response. An enabling code would then be transmitted from the network back to the user radio (and the user) which, when accepted by the user, configures the radio in a proper state to support that user's role. The user would then follow up with command to find out specific details of their actual tasking within the incident.

- Ability to authenticate a user's qualifications, in support of a specific incident need.
- Ability to query user radios for information including, but not be limited to, manufacturer, radio type, available modes, software/hardware version numbers, reconfigurability, etc. The format/protocols for such information must be vendor neutral and standardized. This capability is particularly important when a mix of radio types are being used and not all devices can be pre-programmed.
- Definition of appropriate radio capabilities in context of its user's role. Note this can range from manually defined, pre-planned assignments (which is completed, to a limited extent, within current device capabilities) to a more cognitive-based, dynamic function which operates in conjunction with network management resource allocation (see Use Cases 2 and 3) to dynamically determine and provide appropriate radio capabilities needed to support a user as the incident evolves.
- Ability to associate users, radios, and user roles.
- Ability to reconfigure the radio based on the user's role. There are several approaches to reconfiguration that can provide this capability. The simplest approach is to reprogram the personality of the radio, which includes frequencies, channels, talk group assignments, and so on. This capability is a typical feature of public safety radio systems available today.
    - An additional level of control on radio use could be achieved by also using downloadable executable policies. These policies would define constraints and implement restrictions on the use of the radio based on the responder's role. Use of policies could ensure that the use of the radios stays within regulatory constraints, and also provides additional controls to avoid the challenges of "everybody talking to everybody".
    - Radio capabilities constrain radio reconfigurability. For example, a radio that does not have a P25 data capability is not likely to be able to be "reconfigured" to handle P25 data, given the current generation of P25 radios, without a complete software download or hardware upgrade. However, it may be possible to have capabilities pre-programmed into their radios but selected capabilities disabled for use until reconfiguration activates them. Then, when the radio is deployed in a situation described above, specific required capabilities could then be enabled (turned on) and any that are not required could be disabled.
- For over the air reconfiguration, a standards-based over the air programming capability is needed, to include the software tools and a radio "meeting point" (with standardized modulation, bandwidth, frequency, and protocols) to obtain configuration data for radios to be reprogrammed over the air.
- Sufficient security must be included to ensure integrity of the over the air reconfiguration process.[11]

[11] The Wireless Innovation Forum Security Working Group is currently addressing this topic and is preparing a report entitled "Securing Software Reconfigurable Communications Devices" for subsequent release.

- An ability to restore a radio to a previous configuration, including a default configuration and the re-configuration of the radio to its state prior to the incident; this function is addressed separately in the Revert/Rollback Use Case discussed in Section 5.8.)

5.1.3.2 Regulatory Implications

All channels/frequencies to be used are licensed public safety frequencies. Therefore there are no regulatory implications of this use case for radio use by public safety personnel.

However, the licensee of a given radio may not be licensed for channels which are available and for which a pre-existing mutual agreement is not in place, precluding legal use. Regulatory changes could facilitate this process; for example, use of downloadable executable policies covering frequency usage that reflect regulatory policies could allow more dynamic application of regulatory constraints.

Some regulatory support may be required for implementing the "meeting point" function described in Section 5.1.3.1 for standardized over the air reconfiguration.

However, this use case also facilitates the ability of non-first responders, particularly if they are acting as liaisons to public safety personnel within an incident command framework, to have a role defined such that their radio include public safety frequencies. This aspect of the use case may require some regulatory changes to be realized. (See the Interface with Non-First Responders Use Case discussion in Section 5.6 for a use case discussion specific to the communications interface between first responder and non-first responder personnel.)

5.1.3.3 Policy Implications

The major policy implication of this use case is definition, in much greater detail, of the relationship between radio capabilities and responder roles than is currently available. Note that these policies and procedures will likely vary from jurisdiction to jurisdiction unless national standards are established and followed. One advantage of this use case is that it allows individual agencies to define policies and procedures for incident response, and ensure that responders with whom they have previously trained or worked with can follow those polices since they are programmed into their radios.

Procedures must also be defined to:

- Describe responders' roles;
- Authenticate the users and their assigned roles; and
- Test the radio by sending/receiving a set of test transmissions to ensure that the reconfiguration was properly executed.

Users will need to be trained in the reconfiguration process and changes in radio behavior that may result.

A standard definition of radio capabilities and the protocols used for query/response transmissions must be defined to allow the network to query radio capabilities to determine how the radio can be reconfigured to support the defined role.

5.1.4 Summary of Impact of Use Case

One of the major concerns expressed by the public safety community about interoperability is that providing interoperable communications can devolve into chaos if everyone can talk to everyone. Aside from extensive training and user discipline, one way of managing this issue is to provide responders with the only the communications capabilities that they need without providing them capabilities that they do not need. "Need" is based on the responder's role in the incident response. Thus role-based reconfiguration of radios provides agencies with much greater control of their communications resources and reduces the risk of inefficient use of those communications resources, and eliminating confusion resulting from establishment of links and resources that are not needed or appropriate. Furthermore, individual agencies can define agency specific policies and procedures, in terms of radio configuration, so that responders who typically do not use the network(s) supporting an incident response can operate within these defined policies without significant additional training.

The other significant impact is that role-based reconfiguration provides must greater ability to evolve communications capabilities to meet the changing demands of an evolving incident. One of the challenges in incident management is that incidents are unpredictable and dynamic—no amount of pre-planning can account for all possibilities, and user training is focused on providing an overall framework that can be adjusted as needed. This use case provides tools that allow user communications capabilities to be dynamic, and adjusted as needed to meet incident communications requirements.

5.2 Use Case 2: Resource Management in a Dedicated Public Safety Network

There are several points in the scenario in which real-time management of network resources becomes critical. While network resource management is always an important component of communications support, several events in the scenario (16, 18, 25, 29) highlight specific situations in which incident communications requirements exceed the system capacity, creating a need for greater network resource management tools than are available today.

For example, as the incident progresses the shared broadband network capacity reaches its technological throughput limit. The network moves into its next level of QoS parameters and begins to throttle some types of traffic throughput, particularly for data intensive applications. Applications respond to the throttling by reducing their throughput requirements while still delivering an acceptable product. Traffic cameras sense the reduction in available throughput and reduce the quality of the frame rate of the video. AVL and other sensor data reduce their beacon rate. The commanders notice the reduction and begin to force some sensor applications to send updates more frequently. The applications respond by resetting their beacon rate to a more acceptable level, other less critical sensors, intern, reduce their beacon rate further to compensate.

As the broadband network reaches capacity, the voice network does also. In response to incident needs IC directs FDMA users to use (repeated) conventional national interoperability channels, allowing the trunked system to handle more TDMA users, effectively providing more capacity. Simultaneously a frequency sharing agreement is invoked with Metropolis. The Central City 700MHz trunked system communicates with the Metropolis trunked radio system, to dynamically allocate additional frequencies, as needed, to the Central City system. This agreement allows an extra 5 channels or 10 TDMA talk paths to be temporarily added to the Central City system.

Another potential aspect network resource management involves a concept which we refer to as spectrum mutual aid. In much the same manner that agencies share manpower and equipment resources during major incidents, the ability to reconfigure communications resources could allow agencies to share spectrum resources. Agencies could establish sharing agreements that, by mutual consent, disable use of a particular frequency by one agency (for which it is licensed), and then allow another agency to utilize (borrow) that frequency during a major incident. As noted below, this concept requires some regulatory and procedural changes, and would require appropriate frequency coordination prior to deploying equipment and establishing such a mutual aid pact.

Network resource management may be helpful in adjusting talk groups or other network links as the incident evolves in geographic scope and/or number of users. For example, a traffic perimeter control net may need to be sub-divided into multiple nets as the incident perimeter expands, as voice traffic on the designated channel/talk group approaches capacity, or the geographic extent of the perimeter expands. Monitoring evolving geographic extent of communications is required for an incident and critical to ensure that users stay within the coverage area of the communications channel being used, and that incident transmissions are not disrupting other mission-critical communications at the "edges" of the evolving incident. The proposed cognitive capability described in this case is use of information about the location of the radios, traffic loading, role information (see Section 5.1) and the RF environment (see Section 5.4) to determine optimum allocation of frequency resources, and modification of talk groups, and so on. The most likely implementation approach would involve cognitive capabilities able to recognize (or anticipate[12]) a situation in which communications are likely to degrade, and then recommend solutions to a network operator or comm. unit leader for execution.

Network resource management can also be implemented on a more localized scale; for example, using technology such as adaptive antennas and/or adaptive power output can be used by individual radios, or coordinated among multiple radios in a network to mitigate the effects of RF interference. This topic treated as a separate use case (see Section 5.4).

5.2.1 Summary of Scenario Situation

In terms of the aspects of the public safety communications environment:

1. **Physical:** The extent of the damage caused in the chemical plant explosion requires marking and recording each location that involved casualties, fire, evidence, incident parameters, etc. The affected area, where information must be collected, can extend over a large geographical area encompassing both hazardous and non-hazardous zones. In addition, there are a significant number of first responders located within the immediate vicinity of the chemical plant.
2. **Network**: Network loading approaches the capacity of available network resources. Presently geolocation information is exchanged, via a narrowband channel, on the land mobile radio network (if the feature is available) and the resulting information is not conveniently available to the Incident Commander or Comm Unit Leader. In current trunked radio systems, queuing times for calls can be collected, but this information is not mapped to the location of the communications assets to provide an overall "picture" of

[12] For example, a cognitive capability with information on radio locations, channel frequency, and terrain/land use could run coarse propagation models to anticipate when radios may exit the coverage footprint of a network.

the RF environment. Network management data that is (sometimes) communicated in a standard way from public safety subscriber devices to the network, for network management use (such as channel occupancy) is insufficient to support the scope of network resource allocation envisioned in this use case. In addition, there is no overall control of spectrum requirements for data transmissions that could be varied as a function of priority, resolution, and so on.

3. The exchange of geolocation and RF information by network entities will depend on the degree of interoperability deployed to promote and support the seamless transfer of data. Interoperability enhances operations and saves time; conversely, lack of such interoperability results in inefficiencies which can translate into lost time and affect safety of first responders.
4. **Procedural**: Current procedures provide limited options for network resource management. Talk groups, priorities, and QoS controls can often be modified, but generally they are not because of the difficulties of doing so. This must be done manually, and without all of the supporting data required to do so effectively. Procedures to allow spectrum mutual aid generally do not exist other than for certain pre-established shared channels
5. **Regulatory:** There are several aspects of network resource management which are bound by current regulations.
    a. Reallocation of frequencies: only frequencies licensed to the system user can be reallocated, and only within the licensed footprint of that channel. There is currently no regulatory provision for allocating/loaning licensed frequencies to another user (the spectrum mutual aid concept).
    b. Frequency coordination is often based on defined contours; changes to the contours by adaptive antennas are not allowed under current rules. Using frequencies that are licensed by a user at a specific location, at another location, will often fall outside licensed contours. Regulatory implications become more involved when those contours are in the vicinity of international borders. (Conversely, use of adaptive antennas might also be used to ensure licensed contours are not exceeded).
    c. Geolocation signaling is covered under existing rules for public safety communications.
6. **Chronological:** Network resource management options are limited and generally not automated. When an incident starts, network resource allocation is critical, but it is impossible to predict how the incident will evolve over time, and therefore current capabilities tend toward static network configurations that are increasingly inefficient over the course of the incident. Manual changes to the network, to better allocate resources, require minutes or hours for implementation.

5.2.2 Capability Shortfall

Current (trunked) public safety systems have some limited capability for reconfiguration to accommodate network resource management. Implementing network changes through the use of these capabilities effectively in real time is limited, due to:

- Lack of data (such as locations of user radios and information about the RF environment) that can be used to better configure network resources;
  - Present day public safety geolocation capabilities utilize custom alert messages that the radio can send containing pre-determined events (such as Unit Emergency Alert) or more typically, an IP Service where radios can be polled and then respond with location data (either with a onetime response or a periodic response until time expires and/ or # responses is sent). The PSSIG is not aware of any LMR Air Interface that sends GPS location data embedded with a voice call (i.e. embedded in the header data and therefore capable of being sent regularly all the time, with any voice stream).
  - RF information is not available for analysis or for network resource management decisions, and there are currently no capabilities in place to adjust spectrum demands or to arbitrate among competing communications requirements.
- Limitations in reconfiguring radios to automatically take advantage of changes in the network structure/topology.
- Limitations in network reconfiguration capabilities.
- Lack of effective tools to monitor, anticipate, and identify situations in which network resources should be reconfigured.
- Limitations in automating the network reconfiguration process.

5.2.3 Description of Use Case

As the incident unfolds a cognitive capability within the network monitors the geolocation of the radios on the net, the traffic loading on the channels, and the RF environment as reported by the individual radios. The cognitive capability monitors trends, for example; geospatial distribution of radio users on certain radio nets that remain in the same general area (e.g., users located within the immediate area of the chemical plant) or radios supporting users on other nets (such as those assigned to coordinate evacuations) that cover larger, and shifting, geographic areas. Users on some nets provide a relatively constant level of traffic, while traffic from users on other nets require significant increases in capacity as the incident evolves. The network cognitive capability monitors these ongoing situations, and determines at various points in time that network resources need to be reallocated to ensure coverage (see Section 5.4) for all radio users that are on a particular net/channel, and to ensure that there is sufficient capacity by dynamically re-allocating frequencies, or adding frequencies in support of incident communications, or by changing user priorities (or QoS parameters) ensuring that the most important transmissions have the highest probability of success. These tasks must be completed without causing interference to other networks.

A survey of the explosion area is conducted by LE, Fire, and EMS personnel to mark and record geolocation data of casualties, fires, evidence, the incident perimeter, etc. This information is available to the IC as a GIS overlay on a map of the explosion area. Network operational information (location and operating parameters of radios, detected signal strength information, spectrum sensing data) is also provided to the COML.

The impact of these capabilities is such that information can be collected, analyzed, and disseminated to those with need. The network cognitive capability would provide recommendations for

action and also enable RF environment and geolocation information to be transmitted to the Comm Unit Leader. The Comm Unit Leader uses the information provided to optimize, modify, and then execute recommended network changes, reallocating network resources (power output, talk group assignment, frequency reuse) as needed. With respect to the specific aspects of the scenario situation described in Section 5.2.11, this use case would result in the following:

1. **Physical**: There is no change to the physical deployment of assets. The cognitive-enabled reconfigurable device is deployed in the same manner as current devices.
2. **Network**: Connectivity (e.g., who can talk to whom) would not change. How the network implements connectivity may change, including network aspects such as the allocation of frequencies, user priorities, and QoS parameters. The cognitive capability would be integrated with geolocation information to optimize radio transmit power output, talk group assignment, and frequency reuse.
3. **Procedural**: There are a number of procedural implications that must be addressed in order to realize this use case:
   - COML (or network operator) procedures (and training) would be changed to provide the expertise to effectively manage the network resource management options that would be available.
   - Dynamic allocation of frequencies; before frequencies licensed to agencies are made available (loaned) to other agencies via "spectrum mutual aid" agreements, pre-coordination (via frequency coordinators) will be required to ensure that these operations do not impact third party agencies.
4. **Regulatory**: Some regulatory changes would be required to permit the dynamic allocation of frequencies by non-licensed users per agreements with licensed users. The other aspects of this use case, such as modifying talk groups, cross-programming within subscriber radio units, reassigning channels, and so on are capabilities that are allowed today, but are not generally performed automatically. There are not likely any regulatory changes required to accommodate those capabilities.
5. **Chronological**: Enabling this cognitive capability would increase efficiencies in responding to situations that arise and then subsequently dealing with network changes in support of the response. Native cognitive capabilities would be seamlessly handled. Network reconfigurations that require manual activation are likely to require minutes or hours; cognitive capabilities that can provide recommendations can cut this time to seconds.

5.2.3.1 Functional Capabilities

There are a number of functions that need to be implemented to realize this use case, they are listed below.

- **RF Environment Sensing:** This cognitive capability described assumes a decision process based on knowledge of the RF environment which, in turn, requires that the individual radios provide some information about the RF environment at their location. The specific type of information to be collected may vary based on the algorithms for monitoring, anticipating, and identifying network resource allocation issues (see paragraph below). In general, this would include the received signal strength of the network transmit site, signal-to-noise and/or signal-to-interference ratios, for both the frequencies currently

being used by the device and information about other frequencies accessible by the radio. In addition to an ability within the radio to collect this information, there must be a standard method of transmitting this information back into the network for analysis.

- **Geolocation:** The cognitive capability to use geolocation data is implemented in one of two ways: autonomously and manually. Autonomous geolocation capability is made possible using radios that have this cognitive capability incorporated into the radio devices, infrastructure, and command and control interfaces. This geolocation functionality executes in the background providing information to the network; information that includes user identification data, location data, and radio operational statistics under normal conditions. When the system senses an increase in activity, the network cognitive function will adjust resources to accommodate traffic loading changes and the nature of priority of calls. If a user connects a peripheral device such as a camera, oxygen, or chemical sensor, etc, to their cognitive radio it will automatically begin integrating the new data into the infosphere. On the dispatch or command and control end, the system infrastructure and computer aided dispatch services will incorporate this new information into the network external sensor data pool.

  The second approach to incorporation cognitive geolocation capability is through an interoperability device that cross-patches information between disparate radio systems. Once the system has been manually activated, the device will automatically sense the type of radio networks that are being bridged and information about associated network subscriber equipment, from which it will extract available geolocation information. If interoperability plan data is available in advance, the interoperability device will utilize that information when cross-patching the disparate system. Manual intervention is needed to terminate the use of the manually operated initiation of the interoperability device to utilize geolocation information.

  If this geolocation feature is enabled, when a visiting subscriber device is added to the network, the network will automatically incorporate it in a manner analogous to adding a peripheral device to a personal computer. Device features could be added by downloading device drivers automatically and then to adding data received from the vesting device to the dispatch console. If a specific feature is not supported, the information will be logged or archived for post processing.

- **Algorithms for monitoring, anticipating, and identifying network resource allocation issues:** Core cognitive capabilities include an ability to monitor data from the evolving incident, then establishing trends and trigger points for network changes, anticipation of the need for network reconfiguration, and then identifying available options for COML use. Trend analysis is important to distinguish between network events; e.g., simple short-term spikes in network traffic versus a temporary geographic relocation of network users for which resources must be quickly adapted, or by quantifying longer term trends associated with incident evolution.

5.2.3.2 Regulatory Implications

Some regulatory changes would also be required to permit the dynamic allocation and sharing of licensed frequencies, by other users, per pre-established agreements with licensed users (this is similar to the regulatory considerations described in Section 5.1.3.2). Other aspects of this use case, such as modifying talk groups, reassigning channels, cross programming of frequencies etc, occur within

the rules today, but these network changes are not generally performed automatically. There are not likely any regulatory changes required to accommodate those capabilities.

For network based cross-patching or transcoding of information between disparate (licensed) systems, regulatory requirements should not be an issue because current the over-the-air regulations currently governing these operations would be in force. Non-network based over-the-air transactions would be subject to regulations governing public safety LMR communications.

5.2.3.3 Policy Implications

A major policy implication involves a significant change in the role that the COML, or network operations manager, has in terms of real-time network control. Current systems generally rely on extensive pre-planning and network management generally ensures that the network stays operational within a mostly static network plan. This cognitive use case envisions that a much wider range of options for dynamic network resource management will be available to the COML, or network operations manager. Options supported by data and analytical capabilities that are not available today. Note also that policies may need to be established or modified as to the conditions under which data that could continuously track the location of responders is collected, maintained, and disseminated.

5.2.4 Summary of Impact of Use Case

By collecting RF and geolocation information from individual radios, a COML or network manager would have access to data necessary to more effectively manage communications resources. Management of current network technology relies on static, pre-defined allocation of resources that are difficult to enhance as incident response requirements change. With access to geolocation data, the COML would be able to monitor, plan, and react to changes in the environment and the incident response requirements to utilize communications resources more effectively.

5.3 Use Case 3: Resource Management in a Shared Public/Private Network

The network management use case described above, in Section 5.2, focuses on management of resources assuming a dedicated public safety network. However, one of the elements of the scenario is the existence of a shared public/private broadband network. While there are many similarities in the capabilities needed for network resource management for both the dedicated public safety network and the shared public/private network, we analyze this case as a separate use case because there are significantly different regulatory and procedural considerations (which should be transparent to the first responders).

The motivation for this aspect of the scenario is based on the ongoing activities regarding the 700 MHz spectrum in the United States. Although the final rules governing use of that spectrum were undetermined at the time of this report, the concept of establishing a shared network using common spectrum and common network resources to support both public safety and commercial users is still a potential outcome. A shared network is one that can benefit from both software defined radio and cognitive radio technologies.[13] For the purposes of this use case, we assume that there is a shared

[13] See Forum Reports "Considerations and Recommendations for Software Defined Radio Technologies for the 700 MHz Public/Private Partnership," Report No. SDRF-07-R-0024-V1.0.0, and "Utilization of Software Defined Radio (SDR) Technology for the 700 MHz Public/Private Partnership," Report No. SDRF-08-P-0004-V1.0.0, both available at www.wirelessinnovation.org.

network, in which spectrum resources are licensed for both commercial and public safety use.[14] There is a network sharing agreement between the public safety and commercial entities accommodates commercial use of the spectrum during routine conditions, and prioritizes public safety use of the spectrum during emergency situations. Other aspects of the partnership (regional or national, whether the public safety license holder is the local agency or a national license holder, and so on) are immaterial to the use case.

Event 15 requires the network sharing agreement emergency provisions to activate in the system. The current demands of broadband data to incident command have exceeded the negotiated threshold. The network agreement must mandate automatically reconfiguration of resources to accommodate the bandwidth requirements of public safety users through any way possible. Note that Use Case 2 addresses network resource allocation and network management in general. This use case extends that concept to look specifically at the use case in the context of a shared public/private system.

Based on governance and resource sharing rules, when activated, the cognitive network immediately activates its emergency service plan and places public safety data at the top of the QoS prioritization list. The cognitive network begins to plan for other ways to accommodate user throughput needs, by increasing modulation complexity and/or channel bandwidth. The network must automatically sense the most efficient modulation format available, based on the location of the responders. The network must identify the towers through which the responders and command are communicating. The network may then reconfigure the carriers' frequency reuse plan to increase channel bandwidth on some towers, which may also include disabling some network resources for the duration of the emergency. As responders move, the network automatically optimizes its configuration, as required, to adapt to user needs.

As noted in Event 15 of the scenario, the network resources include terrestrial and satellite communications. Cognitive capabilities can also provide intelligent routing to sustain connectivity when communications links cannot be supported by land-based network segments, because of network capacity constraints, or because user nodes move beyond the RF coverage area of the network.

5.3.1 Summary of Scenario Situation

In terms of the aspects of the public safety communications environment:

1. **Physical:** There are a number of first responders located in the same area as non-first responders (e.g., victims, people trying to evacuate the area, people stuck in a traffic jam caused by the vehicular accident, and so on)
2. **Network**: Both first responders and non-first responders are accessing the shared network resources per the existing network sharing agreement.
3. **Procedural**: The network sharing agreement specifies that under certain emergency conditions, the ratio of network resources allocated to first responder communications and those allocated to non-first responders can be changed, effectively increasing the allocation used by public safety.

[14] Note that this could be established in a manner along the lines of the FCC's original concept for Block D of the 700 MHz spectrum, or through an allocation of spectrum specifically designed for shared use.

4. **Regulatory**: This resource re-allocation is based on a pre-negotiated agreement within the existing regulatory framework.
5. **Chronological:** The need to re-allocate resources is determined and executed over a matter of seconds.

5.3.2 Capability Shortfall

The concept of a public/private partnership in which spectrum allocation can change based on need and an emergency circumstance does not exist to the extent that is envisioned in this use case. There are examples of trunked systems in which public safety and other non-public safety governmental functions co-exist, and there are examples in which public safety users utilize commercial data systems, but neither of these examples reflect the challenges inherent in a network shared between commercial users and public safety users in which network resources are reallocated based on emergency conditions.

5.3.3 Description of Use Case

This use case specifically describes cognitive capability to automatically implement network resource allocation procedures defined in a network sharing agreement between a commercial carrier and a public safety agency.

With respect to the specific aspects of the scenario situation noted in Section 5.7.1, this use case would result in the following:

1. **Physical**: The physical location of the public safety and commercial users does not change in this use case.
2. **Network**: Connectivity remains the same in this use case; public safety and commercial users continue to access the network. However, the resource allocations change as a function of public safety network user needs, establishing a lower priority for commercial user bandwidth needs during incident response, resulting in greater blockage of lower priority commercial traffic during the incident. This condition is a transitory state that will automatically revert as the incident response dissolves, and commercial customers would purchase services based on prior knowledge that commercial network resources are managed in this way[15].
3. **Procedural**: The procedures for network resource allocation are defined in detail in the network sharing agreement between the public safety license holder and the commercial entity.
4. **Regulatory**: The regulatory regime provides explicit support for shared spectrum use.
5. **Chronological**: The procedures for network resource allocation are defined prior to an incident. Execution of the procedures occurs in real time.

5.3.3.1 Functional Capabilities

Functional capabilities required to realize this use case include the following:

[15] Conversely, since the shared network would be build to hardened public safety specifications, commercial customers would likely gain in the context of enhanced day-to-day network reliability.

- A capability to adjust network resource utilization based on the terms of the network sharing agreement. The core cognitive capability is to provide a greater portion of available network resources to public safety when they are needed by public safety. The specific implementation of this capability would be driven by network sharing agreement terms. For example, an agreement would typically provide for public safety use of a predefined portion of shared network capacity on an as needed basis for day-to day operations, requiring some simple prioritization of traffic such that commercial access is on an as-available basis. The network sharing agreement would also have terms by which public safety could utilize all available network capacity, pre-empting all commercial use. If this "trigger condition" is based on a public safety utilization threshold, or some alert condition, then some network load monitoring capability would be required to monitor these conditions and activate network priority changes. If the network sharing agreement relies on some external declaration "trigger" condition(s) have been met, it may still be helpful for relevant data to be collected by the network. It may also help overall network resource management if agreement "trigger" conditions can be anticipated or predicted.
- The capability to revert from public safety network priority use is required as the emergency communications requirements decline below the trigger thresholds. This capability is the inverse of the above capability, and relies on the same network operations monitoring and incident management as the capability to increase the spectrum allocated to public safety. We identify it separately because the ramp down of network operations often tends to not receive the same level of interest as the ramp up process, and because the economic viability of such networks is likely to depend on the rapid restoration of commercial services (consistent with ensuring that public safety operations are not compromised).
- In addition to identifying the key conditions for network sharing, the other function required to realize this use case is the ability to allocate additional spectrum in the most effective manner.

5.3.3.2 Regulatory Implications

The assumption in this use case that "the regulatory regime provides explicit support for shared spectrum use" has not been broadly adopted at this time. In the United States, there has been a lengthy proceeding relating to this concept and the related auction of spectrum in the 800 MHz frequency band. While much of the proceeding dealt with auction rules and licensing (which we do not address here), the regulatory framework of a network sharing agreement between public safety spectrum and commercial spectrum licensees has also been debated in great detail. Rather than repeat that extensive discussion, we note here that currently regulations do not generally support the level of spectrum sharing envisioned in this use case, and thus significant regulatory changes would be required.

5.3.3.3 Policy Implications

There are a number of policy implications related to this use case. The heart of the policy considerations is the proposed network sharing agreement. Such an agreement would codify the policies of spectrum sharing.

For the individual users, however, there would be little policy change required, as the use case involves dynamic allocation of network resources (capacity) for public safety use, most likely in a

network built using shared commercial and public safety spectrum. Thus the only impact to the end user should be improved performance, unless incident conditions cause commercial traffic to be completely pre-empted on the network; a known potential condition, established in commercial end-user service agreements.

5.3.4 Summary of Impact of Use Case

The major impact of this use case is enhanced performance and capacity for public safety users during an incident response. By sharing spectrum resources, public safety users have access to more network resources when needed to support incident response communications, allowing more data to be moved more effectively and quickly, with greater robustness.

5.4 Use Case 4: Coverage Performance Improvement

Event 19 captures the notion of the presence of interference and the ability of the cognitive network and cognitive subscriber units to adjust operating parameters as necessary to mitigate the effects of RF interference as well as improve noise-limited performance. In event 19, RF interference is caused by increased traffic occupying nearby frequencies that are close enough (in frequency and/or location) to public safety user communication channels to cause blockage and/or interference residue via leakage through the radio's filters.

5.4.1 Summary of Scenario Situation

In terms of the aspects of the public safety communications environment:

1. **Physical:** There are a number of subscriber units that must communicate when responding to the hazardous situation, but communications is hindered and even prevented by interference and network signal levels are weak for some users, which causes noticeable degradation in voice quality.
2. **Network**: The network is a typical public safety trunked radio system, consisting of one or more sites where base stations/repeaters are located, network backhaul data links from the sites, networking switching/routing to route radio communications from the source to destination communications devices (subscriber units, dispatch centers, etc.), and all network control and database peripherals. Base stations typically can sense when there is an excessive interference source and disable those channels (a brute force solution that reduces overall system capacity).
3. **Procedural**: The procedure for dealing with interference and poor voice quality due to weak signal is subscriber- and/or base station-centric. If a user's transmissions are not understandable, the user repeats the transmission and/or moves in the hope of getting better coverage. When base stations sense when there is an excessive interference source and disable those channels, this is typically transparent to the end user if other channels are available but it also affects access capacity and latency times. Roaming algorithms are also employed in radios so that the radio can "automatically" try communicating on alternate trunked sites if the received signal falls below a threshold and/or the received BER is excessive. For voice quality to improve, obviously there needs to be coverage overlap between network sites with robust link margins. A more "brute force" technique

than roaming is for the radio operator to manually force his radio to use a different site, system, or even frequency band (rarely happens) in the hope that voice quality will improve.

4. **Regulatory:** The frequencies and waveforms that the subscribers and infrastructure are authorized to use in a given area are dictated by licensing.
5. **Chronological:** Depending on the severity of the interference, the trunked system response time can collapse into a gridlock condition since every repeated transmission represents additional traffic and additional traffic, in turn, further delays response time.

5.4.2 Capability Shortfall

In regards to interference-limited communications, today's trunked public safety base stations typically employ limited interference avoidance on the control channel, using a technique that is often termed "carrier detection". The carrier detection technique discriminates between wanted and unwanted receive signals in the base station control channel receiver using the time domain characteristics of the signal envelope. Desired receive control channel signals originating from radios wishing to communicate with the station will be in short bursts (i.e., on for a short time, then off). If the base station receiver detects that a received signal does not exhibit this characteristic (e.g., it is long duration) and of sufficient level to interfere, it will shut down that channel and the control channel will revert (direct subscribers) to the next available channel.

Roaming algorithms, manually forcing an end users radio to access a different site, or even frequency band changes, as described in the Procedural entry in Section 5.4.1, do not provide high assurance that a weak signal power condition will be corrected. Roaming algorithms can have many thresholds that are often specific to the environment in which the radio operates, and these thresholds must be fine-tuned. Also, a radio operator who manually changes systems during deep fading situations may find that the signal "comes and goes" even after making his alternative signal source selection. As a result, he may find himself having to repeatedly change controls on his radio, thus causing distraction from his life-critical mission.

The current brute force, manual, and subscriber-centric methods of dealing with interference and weak signals are cumbersome, time consuming, spectrally inefficient to say the least, and they can even cause system instability and/or breakdown in severe cases. "Smarter", network-based solutions can improve spectral efficiency via intelligent, optimal, algorithms that can be automated.

5.4.3 Description of Use Case

The interference mitigation and link margin improvement techniques for Event 19 use the known location of both the subscriber units and interference sources, the subscriber units' desired data rate needs (e.g., voice, slow speed data, or high speed data), the subscriber units' priorities, and analytical prediction of the RF coverage to choose the following parameters for each subscriber based on a multi-dimensional coverage, priority, and traffic optimization:

- Transmit power
- Waveform (various bandwidths corresponding to different data rates)
- Frequency channel(s)

- Sites and systems
- Antenna parameters and/or configuration

The information is sent by the network via a control link to each radio and site. Each radio, in turn, adjusts its transmit and receive filters commensurate with optimality for the particular waveform, its power output is configured to be "just enough" for communications at the desired quality of service, its operating frequency set to be far enough away from other radios' communications channels to enable enhanced cancellation by its receiver filters, and its site and/or system if improved coverage is predicted with this alternate selection. Also, if adaptive and/or reconfigurable site and/or terminal antennas are employed, the parameters of such antennas may be changed or adaptively enabled to form a beam in the direction of the desired communications path and/or set a null on the direction of arrival of (a) received interference signals(s). The network also controls network access of each subscriber based on its priority relative to other subscribers.

If the location, bandwidth, power, and frequency of the interference is unknown this substantially increases the complexity of the multi-dimensional optimization, but techniques such as game theory may be applicable to help ensure desirable network behavior in light of the distributed control.[16]

Candidate techniques that can be prescribed by the network when dealing with interference include the following:

- Frequency agility—move the communications channels away from the frequencies where the effects of the interference are being observed
- Burn through—increase the power output of the subscriber units and/or use waveforms that can better tolerate the interference
- Coverage extension—set up an ad hoc network to reduce the ratio of communications range to interferer range, which achieves better signal to interference ratio.
- Subscriber receiver parameter modification—mitigate the effects of the interference by changing subscriber receiver parameters; if the interference is causing a blockage due to overload of the radio receiver, sometimes insertion of additional receiver attenuation will improve the signal to interference ratio.
- Antenna nulling—use site and/or terminal antennas that can place a null in the direction of the interfering signal, either adaptively or via external control.

Candidate techniques that can be prescribed by the network to deal with weak signals include the following:

- Power increase—increase the power output of the subscriber units (for terminal to base station limited situations)
- Waveform design—use waveforms that can better tolerate weak signals
- Coverage extension—set up an ad hoc network to "relay" the signal among closer spaced radios

[16] James O. Neel: "Analysis and Design Of Cognitive Radio and Distributed Radio Resource Management Algorithms PHD Dissertation Virginia Tech September 2006

- Subscriber receiver parameter modification—the optimum receiver configuration in noise-limited situations is typically not the same as for interference limited situations, so in noise-limited cases where adjacent channel interference is not a concern, some improvement in link margin can be afforded with a filter change. Also, even RF front end components of the subscriber radio could be controlled to enable more effective radio sensitivity at the expense of higher interference susceptibility.
- Antenna gain—use site and/or terminal antennas that can optimize gain in the desired direction of communication, either adaptively or via external control.

All of the techniques described in the above lists can be performed today, but require extensive human (manual) analysis. Cognitive radio capabilities can automate significant parts of the process, shortening the time required to execute performance improvement actions and reducing the burden on the humans in the loop. That is, much less time required for operators to react to the situation; operating parameters could be optimized automatically; and automated monitoring of performance over time allows parameters to be adjusted automatically as well. With respect to the specific aspects of the scenario situation noted in Section 5.4.1, this use case would result in the following:

1. **Physical**: There is no change to the physical deployment of assets, except for potentially a more capable network processor to accommodate the network-based application that performs the processing algorithms.
2. **Network**: The existing network will be augmented with an application that implements interference mitigation and/or link margin improvement algorithm(s), and may require additional control interfaces from/to the subscriber units.
3. **Procedural**: Manual operations required with current technology would be replaced by reviewing (and approving as necessary) the reconfiguration steps taken by the cognitive-enabled network.
4. **Regulatory**: Radios are licensed to operate with more waveforms that have more varying bandwidths and data rates. Radios are also licensed to utilize frequencies allocated to other services under specified conditions.
5. **Chronological**: The time required to respond to interference and/or weak signals is reduced significantly.

5.4.3.1 Functional Capabilities

The functional capabilities required to realize this use case include the following

1. GPS in all subscriber units and communication of the position coordinates of each subscriber unit to the network application.
2. The ability of each subscriber unit to specify, to the network application, the subscriber units' data rate needs for its next transmission or message sequence.
3. The ability of each subscriber unit to rapidly change transmit power, waveforms, frequencies, filtering, and receiver attenuation based on commands sent over the network.
4. A network application that includes
    a. A coverage and interference model that can predict signal and interference levels at every potential end-user location.

b. A CR algorithm that optimizes the following variables based on predicted signal and interference levels for all subscribers:

- Transmit power
- Waveform for communication (various bandwidths corresponding to different data rates)
- Frequency channel(s) for communication

c. Dynamically controllable access priority per subscriber unit

5. The ability to set up an ad hoc network[17]
6. Optional adaptive and/or externally controllable antennas for the sites and/or terminals that can place additional gain in the direction of the desired communications and/or nulls in the direction of interference sources.

5.4.3.2 Regulatory Implications

To enable the most "hooks" for improving performance, radios will likely have to be licensed to operate with the flexibility of using multiple waveforms that have more varying bandwidths and data rates. Also, if the cognitive algorithm is extended to "borrow" frequencies from other services this, of course, impacts regulatory procedures/certifications.

5.4.3.3 Policy Implications

The additional functionality of a cognitive network may allow some changes to existing policies and procedures to expedite the deployment of such devices in emergency situations.

5.4.4 Summary of Impact of Use Case

"Smarter", network-based solutions improve spectral efficiency via automated, intelligent, and more optimal algorithms.

5.5 Use Case 5: Reconfigurable RF Gateway Capability

In events 13 and 14 of the scenario, a situation arises in which it becomes necessary to establish a voice communications link between first responders and personnel that do not have access to first responder equipment. For example, tow truck operators need to coordinate their activities with incident command staff and to obtain personal protective equipment (PPE) so that they can go into a hot zone to remove vehicles that are blocking traffic routes that are needed by emergency vehicles.

In this use case, a reconfigurable repeater is deployed to link a frequency used by tow truck operators with a frequency used by the first responders. For ease of reference we refer to such a device as a Mode Agile Gateway Network Enabled Technology (MAGNET) in subsequent use case discussions.

[17] See Use Case 1, Section 4.3.1., "Use Cases for Cognitive Applications in Public Safety Communications Systems Volume 1: Review of the 7 July Bombing of the London Underground," Report No. SDRF-07-P-0019-V1.0.0, 7 November 2007, available at www.wirelessinnovation.org.

5.5.1 Summary of Scenario Situation

In terms of the aspects of the public safety communications environment:

1. **Physical:** There are a number of tow truck operators whose activities must be coordinated within several elements of the response; they must be directed to locations to receive PPE; they must then be directed where to go to remove vehicles, etc. The area from which vehicles must be removed is within a hazardous material plume. The geographic area covered by the responders who need to be connected is generally the immediate area of the incident—an area of approximately 1 mile radius, requiring voice radio links back to the EOC.
2. **Network**: The tow truck operators have legacy equipment that does not operate on public safety frequencies; thus they have no means for direct voice communication with first responders. With current technology, it is possible to deploy a programmable gateway device that could be used to establish the necessary communications link via channel audio bridging.
3. **Procedural**: Assuming the use of a programmable gateway device, the current procedures are for a Communications Unit Leader or other qualified individual to set up the device, determine the parameters of the channels to be connected, and establish the connection.
4. **Regulatory**: Two or more mobile or portable radio units are typically interconnected via an audio gateway bridging device, and these radio units actually provide access to RF channels. The regulations that apply to such radios are in force.
5. **Chronological:** The time required to set up and properly configure a programmable gateway device varies with the complexity of the RF environment, characteristics of the interconnected radio networks, and the experience of the gateway operator. While it is possible to set up and connect two radios in a matter of minutes, experience has indicated that it can take much longer to adjust parameters to ensure adequate quality in the communications.

5.5.2 Capability Shortfall

Using current technology, the typical approach to providing this gateway capability is to deploy a programmable gateway device that patches audio from a radio tuned to a communications frequency used by the tow trucks with audio from a radio tuned to frequency used by the first responders. The gateway manages all radio push to talk controls. There are several different products and approaches that are currently available, including:

- Mobile or fixed-site repeaters that simply retransmit incoming calls on a different outgoing channel.
- Dispatch console patches or audio linking devices (including IP-internetworking devices) that link channels of different radio systems. Such patches are generally permanent capabilities of the network infrastructure rather than capabilities that can be deployed at an incident.

- Intelligent gateway devices that allow a user to define which channels are to be linked together, and can support multiple simultaneous "conversations" through the device.

All of these approaches are characterized by the fact that a radio transmission on one channel must be rebroadcast on each other channel that is linked through the repeater/patch/gateway device.[18]

While such devices are employed extensively today and provide needed communications interoperability, field experience has indicated a number of challenges with the current technology:

- Such devices require personnel with extensive training to operate effectively.
- While set up can occur quickly, there are typically a number of parameters which must be adjusted to ensure effective operation at the time of activation. Determining the optimum parameters and adjusting them can be time-consuming, labor intensive, and potentially tie up valuable communications channels.
- Improperly deployed devices can have a severe detrimental effect on overall communications, and on resources associated with all interconnected networks.
- Mobile devices and supporting networks are susceptible to "parallel" links and loops if more than one gateway is active in an incident.
- All programming is manual; thus if changes need to be made to the gateway device to accommodate changing communications requirements, or changes in RF environment, the device parameters must be manually adjusted.

5.5.3 Description of Use Case

The concept of this use is a gateway device that functions much like current gateway devices, with three notable exceptions: (1) rather than plug existing radios into the device (as required by most current devices), the device has front end reconfigurable transceivers (radios) that can configure to the required frequencies, protocols, and other operating parameters, potentially eliminating the need to bridge at an audio level by bridging at a digital level or at an intermediate frequency ; (2) cognitive capabilities can determine how the radios need to be configured, and (3) the device can monitor ongoing communications to adjust operating parameters to maintain optimum quality of the communications links.

With respect to the specific aspects of the scenario situation noted in Section 5.5.1, this use case would result in the following:

1. **Physical**: There is no change to the physical deployment of assets. The cognitive-enabled reconfigurable device is deployed in the same manner as current devices.
2. **Network**: There is no change to the network. The cognitive-enabled reconfigurable device established the same network connectivity and the same users are connected as with current devices.

[18] We also recognize that with current technology it is also possible that an emergency management coordinator could contact individual tow trucks via commercial cell phone. While that is a feasible approach, it is difficult to broadcast information to all tow truck operators simultaneously, or for individual operators to be aware of what other trucks are doing, etc.

3. **Procedural**: Because of the greater capabilities of the cognitive-enabled device, some changes in the procedures are appropriate. In particular, manual operations required with current technology would be replaced by reviewing (and approving as necessary) the reconfiguration steps taken by the cognitive-enabled device.
4. **Regulatory**: The actual use of the communications channels does not change, so no regulatory changes are required for that aspect of the use case. However, the replacement of separate radios with a reconfigurable transmit/receive capability that is an integral part of the device would typically require that the device undergo the certification required of other radios. This use case assumes that all use of communications frequencies falls within the bounds defined in the licenses for use of that frequency.
5. **Chronological**: The time required to properly deploy the gateway device is reduced significantly (from as long as several hours to a few minutes).

5.5.3.1 Functional capabilities

The functions required to realize this use case include the following:

1. Cognitive capabilities to identify operating parameters of communications links to be connected. Such operating parameters include, but are not limited to, frequency, bandwidth, PL tone, repeater hang time, repeater squelch tail, transmit power, etc.
2. Reconfigurable multiband radio modules that are components of the gateway device. Reconfigurable parameters include those listed above.
3. Elimination of the need to bridge at a baseband audio level by bridging at a digital level or at an intermediate frequency. Encrypted digital signals can be bridged without compromising transmission security at within the bridge, potentially allowing end-to-end encryption between compatible systems.
4. Cognitive capability to identify the degradation of performance, “ping pong effects” when bridging conventional repeaters, or situations in which a channel is “locked up” due to improper parameter setting, etc.
5. The ability to pass authentication and credential information from one system to another through the gateway. Note that procedures are defined in the P25 ISSI to accomplish this, but gateways linking non-P25 systems, and gateways which convert transmission to audio baseband do not have this capability.

There are a range of architectures for a MAGNET device. The majority of devices currently commercially available use an architecture in which radios are connected to the device, and generally switch audio at the baseband level, with some modifiable parameters to control some aspects of the transmit/receive functions. The cognitive functionality for such a device would monitor performance and modify these parameters. Alternative architectures can incorporate reconfigurable transceivers in the MAGNET itself, in which case the cognitive capabilities can control parameters in both the transceivers and the switching mechanism. Regardless of the architecture, the key required functions determine what reconfiguration options are available (whether they involve reconfiguring a radio connected to the device or a programmable transceiver embedded in the device) and what changes are appropriate to improve performance.

5.5.3.2 Regulatory Implications

A reconfigurable gateway device would include reconfigurable radios, designed to operate with specified parameters but able to be reconfigured as needed to replicate different capabilities. Thus the key regulatory issue is how the reconfigurable radio capabilities are certified.

5.5.3.3 Policy Implications

Most agencies have established, or are establishing, policies and procedures governing the use of gateway devices. Some policies may cover guidelines or rules defining the authority and circumstances under which such devices can be deployed, establishing rules for coordination when such devices are to be deployed, and establishing the qualifications of device operators. Such policies and procedures would still be appropriate in this use case. The additional functionality of a cognitive-enabled reconfigurable gateway device may allow some changes to existing policies and procedures to expedite the deployment of such devices in emergency situations.

Also note that reconfigurable gateways are intended to provide communications capability among users that do not typically communicate with each other. It is important to ensure that where possible, users are trained in best communications practices (e.g., plain English) needed for efficient communication of information. In cases where disparate user groups must communicate in emergency situations for which they have not trained, a short list of guidelines should be available and quickly communicated to all users of a linked channel. For example, it is important for non-public safety personnel in such a situation to practice good radio discipline to avoid straining system capacity. Ensuring the ability for disparate user groups to communicate is not only a technical issue but also a training and operations issue.

Policies and procedures must also be established for authenticating users who are on a system that is linked via the MAGNET.

5.5.4 Summary of Impact of Use Case

The positive results of realizing this use case are as follows:

1. Such devices could be deployed with much less time required for the operator to interact with the device relative to current technology.
2. Operating parameters could be optimized automatically if device receive frequencies are known, in addition to the ability to identify transmit frequencies (i.e., the FCC Part 90VHF band does not use paired channels).
3. Automated monitoring of performance over time allows parameters to be adjusted automatically as well. Optimized operation would ensure that the communication link problems such as repeater interference problems, channel “lock ups”, and interference, can be addressed in real-time rather than requiring manual intervention.

5.6 Use Case 6: Interface with non-first responders

In event 27 of the scenario, additional specialty agencies begin to arrive and their radios must be integrated into the networks. Of particular concern are the industrial firefighters brought in from outside the area (and for which there are no pre-existing aid agreements) to assist in controlling and extinguishing the fire. Audio patches (such as a reconfigurable gateway as described in Section 5.5)

are configured for use by environmental health and safety agency personnel. We assume that the industrial firefighters' radios are state of the art and are automatically reconfigured to operate on Central City's network. The COML authorizes the additional agencies to access the Incident Area Network (IAN). The IAN automatically reconfigures its operation to accept the additional client units. Reconfiguration occurs in two ways;

- Reconfiguration of industrial firefighter radios that can be authenticated into the network. For radios that can be reconfigured to operate on the public safety network, those radios are reconfigured in accordance with the roles for which the firefighters are assigned; this situation is similar to that described in Use Case 1 (Section 5.1), with the exception that the personnel in this case are not part of a first responder agency.
- Second, for health and safety agency personnel that cannot be directly authenticated to the network, and/or have radios that cannot be reconfigured to operate on the network, a MAGNET (see Section 5.5) is deployed to provide a gateway interconnecting those firefighters radios and the public safety radio system.

In both situations, the technical aspects of this use case are similar to Use Cases 1 and 5; however, the procedural and regulatory implications of this use case are different. In addition, since the industrial firefighters and health and safety personnel are not first responders, it is also critical that the network connections that allow them direct communications with first responders do not adversely impact the remainder of the communications capabilities being used by other incident response personnel.

5.6.1 Summary of Scenario Situation

In terms of the aspects of the public safety communications environment:

1. **Physical:** There are a number of responders (Industrial Firefighters, Environmental Health, and Worker Safety) that must communicate on the IAN as they work in proximity to the incident area.
2. **Network**: Though the Industrial Firefighters are equipped with compatible public safety radios, they must work through the COML to be authorized on the system. Health and Safety personnel have legacy radios that do not have access to the public safety frequencies and thus have no direct access to First Responders. The COML authorizes use of the MAGNET system to allow Health and Safety personnel to be bridged onto the network.
3. **Procedural**: Two procedures are involved in this instance. First, for the Industrial Firefighters and the Health/Safety Personnel; assuming that the Industrial Firefighters have compatible radios, the process will be for the COML to get information on these radios so they can be authorized on the Central City Network. Assuming theses radios are standards based OTAP capable, the COML will load these radios with the correct template and the radios can be immediately used. Second, in the case of the health/safety personnel, the procedure is much like for the tow-truck; the COML will authorize the MAGNET system to configure itself to accommodate bridging in the Health/Safety personnel into appropriate talk groups as per ICS On-Scene Commander guidance.

4. **Regulatory:** The frequencies and waveforms that the subscribers and infrastructure are authorized to use in a given area are dictated by licensing. Non first responders cannot access public safety systems.
5. **Chronological:** Two separate timelines are involved. The first is the time required to set up and properly configure a MAGNET unit; the required time varies with the complexity of the RF environment and the experience of the operator. While it is possible to set up and bridge two radio systems in a matter of minutes, experience has indicated that it can take much longer to adjust parameters to ensure adequate quality in the communications. The alternative, in which non-first responders such as the Industrial Firefighters have radios that are compatible with public safety systems, is that the interface between first responders and non-first responders could be accomplished with over the air programming once such action is authorized. In this case the reconfiguration timeline is on the order of a few minutes. (Note that in the latter case there is additional time required to add such users as authorized users to the system.)

5.6.2 Capability Shortfall

The capability shortfalls for this use case are identical to the shortfalls listed in Section 5.1.2 and Section 5.5.2.

5.6.3 Description of Use Case

The concept of this use case is twofold. The first is using OTAP to reconfigure the compatible (Industrial Firefighter) radios. The second is to utilize the previously mentioned MAGNET unit which: (1) rather than plug existing radios into the device, the device has front end reconfigurable radios that can configure to the required frequencies, protocols, and other operating parameters; and (2) cognitive capabilities to determine how the radios need to be configured.

5.6.3.1 Functional Capabilities

The functional capabilities required to realize this use case are those listed in Sections 5.1.3.1 and 5.5.3.1.

5.6.3.2 Regulatory Implications

The most significant regulatory implication is that this use case assumes that non-first responders will be transmitting on frequencies allocated for public safety service. While regulations may allow such communications in emergency situations, they may need to be modified to explicitly define the circumstances and appropriate authorizations that should be in place to ensure that such communications is available when needed while not adversely impacting other first responder communications.

5.6.3.3 Policy Implications

Policies and procedures may need to be defined to outline agency rules on the circumstances under which non-first responders can communicate on first responder networks, policies and procedures for authorization and authentication, and policies and procedures for how agency communications assets may be configured to accommodate interface to non-first responders.

5.6.4 Summary of Impact of Use Case

In certain circumstances, such as the ones outlined in the scenario, direct communications between first responders and non-first responders provides more efficient and effective communications. Relaying messages through dispatchers, as an alternative, is subject to errors, takes valuable time, and involves the time and attention of another person (the dispatcher). Other alternatives (such as assigning a liaison officer to work with the non-first responders) require additional personnel for relaying messages rather than performing a more direct incident response task. While the public safety community justifiably is wary of untrained non-first responder use of valuable first responder communications assets, under the appropriate circumstances this use case can provide critical, timely communication that maximizes the support provided by non-first responders.

5.7 Use Case 7: Revert to Previous State

Radio users reconfigure their radios to return to their default home template. As the loading on the voice network lessens, the voice network releases channels back to Metropolis and restrictions on FDMA users are removed from the radio system. The IAN continues to reconfigure itself as responders stand down, units move and leave the network, until there are no more units left to communicate. The broadband network continues to automatically reconfigure itself until utilization drops below specified thresholds. Once below the threshold the network returns to normal operation. A conventional repeater is on site which is able to receive and transmit on multiple frequencies at the same time. The repeater automatically senses the RF environment and allows the COML to create groups of uses through that repeater.

This cognitive capability could reside with the infrastructure, within the radio, or both. If in the infrastructure then the radio would have to be capable of providing this data to the network before it is reprogrammed. If a part of the radio the user might have to tell or configure the radio to save its current state and programming so that it can be restored later.

5.7.1 Summary of Scenario Situation

In terms of the aspects of the public safety communications environment:

1. **Physical:** As first responders arrive at the incident (and throughout the course of the incident), their radios are reconfigured to meet incident needs. The first responders are physically distributed throughout the incident area, including evacuation areas and perimeter control areas removed from the actual chemical plant where the initial explosion occurs. Two potential rollback applications: at some point in the scenario, a reconfiguration of the system (network and subscriber radios) results in a degraded communications capability, therefore these configurations must be restored to their previous state (Use Case 7a). Later, when the first responders are released from the incident, prior to departing for their home jurisdictions, which may be hundreds of miles from the incident, their radios should be normalized , or “rolled back” to a pre- incident, or “home” configuration (Use Case 7b).
2. **Network**: The first responders are linked to the network as needed to support the incident response. At one point the network and subscriber radios are reconfigured, and the result is a degradation of communications capabilities. To resolve this condition, the previous configu-

ration must be restored. Later, some first responders are released from the incident and as they depart their radios are disconnected from the network.

3. **Procedural**: At some point in the scenario the procedure for reconfiguring some element of the communication system (network and subscriber devices) is executed. The result is that communications are degraded.
4. **Regulatory:** The regulations that govern commands for reconfiguration (see Section 5.1.1) apply to this use case.
5. **Chronological:** Current capabilities do not provide simple approaches to systemically roll back changes to configurations. Thus the timeline requires manual review of the communications situation and execution of reconfiguration commands to restore a previous configuration.

5.7.2 Capability Shortfall

For the situation in which a reconfiguration needs to be rolled back, networks and subscriber devices may maintain a configuration history which allows previous configurations to be restored. However, rolling back a configuration change that involves the network and subscriber equipment is not typically automated in current systems. Thus changes which turn out to have a negative impact on communication can only be reversed by manually resetting software configurations installed in the network and in subscriber equipment.

In the case of restoring default or home agency configurations as a responder is released from an incident, the most significant shortfall is associated with radios which cannot be reconfigured over the air. Reprogramming radios that must be tethered to programming hardware can take a significant amount of time (days or weeks) due to the logistics of transporting radios to where they can be reprogrammed. Radio security is not discussed here, but some LMR manufacturers require use of special hardware or software keys prior to accessing radio configuration functions.

5.7.3 Description of Use Case

With respect to the specific aspects of the scenario situation noted in Section 5.7.1, this use case would result in the following:

1. **Physical**: There is no change to the physical deployment of assets.
2. **Network**: Once a network operator or COML issues the appropriate command, the network automatically restores the previous, or home, configuration of the network and the subscriber radios.
3. **Procedural**: A procedure must be in place to determine when a reconfiguration results in degraded communication. This could be an automated process but would logically include some human oversight to avoid unnecessary configuration changes. For visiting users providing mutual aid, the “home configuration” must be stored in the network or on the radio unit itself, for later recall and activation, prior to departing the incident scene. This “image” could be encrypted prior to storage to protect the integrity of the home network, making it unreadable by incident personnel, or to provide a capability to bypass home network security keys. This will also provide significant cost savings for home network personnel.

4. **Regulatory**: No specific regulatory changes are needed to implement the concept of reverting back to a previous state. Some standardization of appropriate messages may be necessary to maintain interoperability in a multi-vendor or multi-model environment.
5. **Chronological**: The time required to reconfigure network equipment, or to rollback a reconfiguration, can be significant if the process is not automated. It can also be a time consuming process to restore subscriber equipment to default or home jurisdiction configurations after the radios have been reconfigured to support an incident response outside of the agency's home jurisdiction. Much of the time in this situation is based on tethering radios physically to programming hardware, a process that can be eliminated with over the air reconfiguration.

5.7.3.1 Functional Capabilities

The functions required to realize this use case include the following:

1. The ability to recognize when a reconfiguration process results in a degraded communications condition. Note that the process of determining that such a condition exists could be entirely manual (i.e., strictly based on the reaction of users or observations of a network operator or COML staff). However, given a capability in which subscribers can report RF information to the network (see Section 5.4), it is also possible that a cognitive capability within the network could monitor RF information and configuration changes to correlate changes in system capabilities and effectiveness of configuration changes. Such information could be analyzed over time to develop more effective configuration options (a "learning" capability) or at least alert a human operator if communications capabilities degrade following a configuration change.
2. The ability to retrieve and securely store prior configuration information.
3. The ability to restore a configuration.
4. The protocols and algorithms to ensure that all radios rollback the correct known and valid prior configuration.
5. The ability to securely return network equipment to a default configuration, via over the air command or reprogramming.

5.7.3.2 Regulatory Implications

No specific regulatory changes are needed to implement the concept of reverting back to a previous state. Some standardization of appropriate reconfiguration messages may be necessary to maintain interoperability in a multi-vendor or multi-model environment.

5.7.3.3 Policy Implications

There are a number of policies and procedures that are required to realize this use case. This use case assumes some level of human oversight into execution of reconfiguration and rollback commands, so the policies and procedures must be put in place to address the following:

- Under what circumstances is a rollback decision made?
- Who has the authority to order a roll back to previous state?

5.7.4 Summary of Impact

Many of the use cases discussed in this document involve reconfiguration of the network and/or reconfiguration of subscriber devices. While thorough analysis, careful implementation, and rigorous testing are mandatory prior to any deployment of such capabilities, the unpredictable nature of real-time incident response means that it is necessary to have contingencies in place, should the outcome of network equipment and/or system reconfiguration not provide the desired or expected results. In such cases it is necessary to return the equipment and/or system back to a known working state as quickly as possible. Current systems do not provide the tools to systematically reverse a sequence of reconfigurations among network and subscriber devices. This use case simplifies this process by providing capabilities to restore a previous configuration as needed.

5.8 Use Case 8: Cognitive Sensor Network

Discussion of sensor input arises in events 6 and 26 of the scenario. Consideration is also given to vehicular traffic in events 13 and 14.

The primary legacy source of automated sensor data is in the personal protective equipment (PPE) worn by firefighters entering the hazardous area. Other related information is typically relayed over voice channels. In exploring the benefits of cognitive capabilities to more effectively respond to this type of situation, we will address additional sources of sensor data, consider how information from them is delivered to IC, and how it is used in the response.

5.8.1 Summary of Scenario Situation

1. **Physical:** A facility with substantial quantities of flammable and potentially toxic chemicals has experienced an explosion and fire, and the situation is out of control. There are two categories of hazards at the site. The first set is associated with physical hazards to personnel entering the area to deal with the fire. The other hazard is presented by a toxic plume emanating from the scene that threatens the nearby population and facilities. Some aspects of these problems can be determined by observation, but others, such as carbon monoxide are invisible, and require sensors to ascertain the level of toxicity. In the described scenario, the primary source of sensor data is from sensors in the protective equipment worn by firefighters. That data relates primarily to the onsite problem, and does not deal adequately with the larger toxic plume that extends beyond the plant location.
2. **Network**: Part of the gear carried into the fire consists of radio equipment providing communications support between IC and other first responders via the trunked radio network. The sensors also generate traffic that requires bandwidth on the IAN for delivery to incident command. Each data radio connects directly to a common central unit. As more firefighters are deployed, sensor traffic increases creating a congestion problem both from the quantity of data generated and the loss of effective bandwidth due to contention for channel time.
3. **Procedural**: Firefighters control when they transmit on voice channels, and can respond to congestion by reducing the number of transmissions and their length. Autonomous uncoordinated sensors, however, are not directly controlled, and lead to channel congestion, with some information that is ultimately redundant.

4. **Regulatory:** Spectrum is assigned to public safety operations, but additional channel capacity may be required to handle the increasing volume of data and voice traffic. There are no unresolved regulatory issues.
5. **Chronological:** During the initial phases of the incident, any issues with hazardous conditions are unknown. Initial notification of a specific hazard is critically important, but repeated messages reporting no change in the situation are redundant, and wasteful of bandwidth. Once existence of a hazard is known, then changes in its intensity or location become relevant.

5.8.2 Capability Shortfall

There are three significant areas of shortfall that can be alleviated by improved system design and application of enhanced information technology. One is inadequacy, or lack of, of available sensor information. Legacy operations depend largely on facilities that responders bring to the scene, and do not take full advantage of supplementary information sources.

Another shortfall is congestion in the communication systems, caused by delivery of information by individual sensors operating independently, and without a coordinated priority structure. This problem can be alleviated by coordination between on-scene CR terminals that cooperate at the data source to avoid data transmission that is irrelevant or redundant.

The third shortfall is onsite information overload on the part of the response team. Both the processing and presentation of available sensor data should provide all needed information in a form that is easy to understand. For example, an on-screen map of the factory, with color-coded symbols to display the hazard level in different areas, is more readily assimilated than a printed list of coordinated and raw sensor data.

5.8.2.1 Supplementary Sources of Sensor Data

The following are additional sources of sensor data that have potential to be processed to enhance overall situational awareness.

A. **Personal Protective Equipment Mounted Supplemental Sensors.** Existing PPE resources provide data from sensors, including life signs data about the wearer and information about ambient conditions, such as air temperature and carbon monoxide levels. To supplement sensors mounted directly on individuals, devices called “pebbles” or “motes” can be placed in the environment. These small radio-equipped devices are dropped at various locations along the path of response both to provide extra sensor data and also augment the communications network.

B. Building Mechanical and Emergency Systems. Buildings are equipped with systems to provide heating and cooling. Those systems have sensor networks with sensors located throughout the building, and the resulting data is used to control building air flow and temperature. The buildings also have emergency system sensors that detect over-temperature conditions, sound alarms, close fire doors, and activate sprinklers. All of these facilities are normally managed via a sensor management or telemetry system centrally within the building, but this control function can often be redirected to external fa-

cilities during the emergency[19]. Sensor power is normally provided via the building power system, but critical sensors can be equipped with battery backup. Data from these sensors can be redirected from the building management system to incident management and/or individual first responders by cable or a local RF network.

C. **Environmental Measurement Facilities.** The US Weather Service has an extensive network of devices that provide meteorological data on a continuous basis. It also provides current weather data summaries and forecasts to predict future weather conditions. The service tracks frontal movement, information that could be used to predict wind shifts that will affect smoke and toxic plume clouds around the scene of an emergency. Additional environmental information is available from other local sources, such as airports and sewage treatment facilities.

D. **Video Cameras.** Video from privately owned and municipal cameras can be used to enhance situational awareness. Due to the amount of information available, video feeds would be recorded at the Emergency Operations Center (EOC), a permanent central site, and edited to select the most relevant footage. The resulting clips are made available to units on the scene when relevant or on demand. Edited and tailored time-lapse information about a plume is an example of preparing video information for maximum effectiveness.

E. **Commercial Digital TV.** With conversion to Digital TV, commercial stations have a 20 MB pipe, more capacity than is needed to deliver their primary program material. With high-powered licensed transmitters these stations have excellent coverage. In an effort to provide additional services, the TV broadcast industry is looking for business cases where a revenue stream can be derived from broadcast of data. Transmission of video content or advertising directly to cell phones, based on geolocation, is a commercial version of this capability.

   For Public Safety, this data stream can supplement dedicated channels for delivery of information from government agencies and other sources. Local municipal or remote FEMA command posts, for example, might use such a channel to download lower-priority but relevant data that might overload busy lower-capacity dedicated channels.

   Commercial TV stations are also generating video relevant to certain types of disasters for use in their news broadcasting, via feeds from cameras located in news helicopters, for example. Their broadcast data sub-channel is a potential way that information, supplementing the video feeds mentioned in D. above, could be delivered.

F. **Cellular System Traffic Information.** The incident generates variations from the normal call traffic patterns as indicated by call volume data and the pattern of hand-offs between cell sites. Geolocation data can be obtained via mobile phones equipped with GPS capability or by triangulation from network base station antennas. This information is used to determine where people with active cell phones are located and to derive traffic patterns in the vicinity of the incident.

G. **Intelligent Traffic Systems.** ITS Cognitive Radios in vehicles, and infrastructure associated with highway automation systems serve as sensors for traffic flow information

[19] See Alan Vinh, Computer-based Monitoring for Decision Support Systems and Disaster Preparedness in Buildings, IMETI Proceedings, June 2008, Orlando, FL

used by Incident Management personnel, including routing of emergency vehicles to the scene. Conversely, information from the incident is used by the highway system to warn drivers and to divert traffic around congested or dangerous roadways.[20]

5.8.2.2 Information overload

When a small number of sensors are active in a given area, routine network query and sensor response data volumes will be small, and channel contention will not present a problem. Both sensor network message volume and network contention will increase issues as data collected from sensors and sensor query activity levels increase while network resources remain constant, significantly more so if conditions trigger transmission of asynchronous alarm data.

In a simple implementation, sensors will repeatedly transmit their current readings to the central system, asynchronously or in response to a system query. A large number of messages with negative reports may not represent useful data. When some pre-defined level of a sensed parameter is detected, that change in status becomes useful information. For example, if a significant number of individual sensors mounted in responder PPE which are located are in close proximity to each other, they may all contend for channel capacity to transmit redundant information, all reporting the same condition.

The solution lies in coordinating information delivery to minimize channel contention. It is also useful to vary reporting intervals to minimize redundant information, while reporting often enough to establish that connectivity has not been lost.

5.8.3 Description of Use Case

This Use Case involves both inclusion of additional sensors as supplementary sources of data, and management of the resulting information. Networks, communication facilities, and operating procedures are modified to encompass the seven sources of information described in Section 5.8.2.1. Activities in the Central City EOC are brought into the scenario.

This Use Case treats the two components of "Cognitive Radio" independently. Cognition is composed of information processing, decision making, and policy execution delegated to the system. Radio is delivery of data of all kinds over wireless links. The Use Case does not confine itself to cognitive functionality implemented in the same box as the RF components: that functionality can be accomplished anywhere in the system. With efficient communication links, data can be processed locally, or sent to remote sites and the results returned with minimal delay.

The following aspects of the scenario situation noted in Section 5.8.1 describe this Use Case:

1. **Physical**: The physical aspect of the scenario is essentially the same as described is 1.1.1., with the addition of traffic sensing as indicated in items F. and G. Some additional equipment, including additional radios and the pebbles, is added. Activities, particularly handling video information, in the Central City EOC result in its inclusion in facilities involved.

   It is of particular interest that significant improvements in capability and performance are realized by the addition of CR functionality with minor physical modifications.

[20] This is an interesting example of system interaction. Two independent systems, developed without a requirement to coordinate, link up and work together to satisfy needs of both DOT for highway management and PS in responding to the incident. Upon conclusion of the event they will disconnect and resume independent operation.

2. **Network**: Network changes to implement enhanced sensor capability are as follows.

A. Sensor communication facilities in individual PPE equipment interact to form an ad hoc network. This net reduces contention, and improves connectivity. In addition, the pebbles dropped by firefighters on their path into the scene contain radios that enhance network connectivity and also provide additional sensors.

B. Building HVAC systems are designed to accommodate an interface with emergency services. A building control diagram is maintained in the municipal emergency information database, and the building network can be accessed for emergency control of the facility. Primary connection to the building network is IP through the commercial service provider data facility, with local wireless backup via unlicensed spectrum.

Individual sensors in the facility connect with the building control room through a wireless local net. Security information needed to access that network is also available to the emergency crew so that sensors can be read out even though the central site is not functional due to the emergency.

C. Meteorological data is important is cases where wind velocity and air temperature influence the plume emitted from the site. The US Weather Service offers a special service for Public Safety use where local weather conditions and forecasts are available for specific locations. The specific location for which information is needed can be obtained from the emergency database, or read from an onsite GPS receiver. In this scenario, the wind shift in Event 32 is forecast. Delivery of this weather information to IC occurs over a DTV data sub-channel from a local TV station.

D. Central City has a number of video cameras available throughout the city. During an emergency these cameras can be controlled from the City EOC to provide relevant incident information, such as information to IC for traffic congestion and plume tracking. Due to the vast amount of footage generated, the video streams are all digitally recorded for computer storage. A feed directly to IC can be provided. Alternately, EOC personnel are trained in both interpreting pictures and editing time-lapse clips which are then transmitted to the IC location.

E. As previously mentioned, commercial TV stations can provide data sub-channels on a contractual basis for emergency use. They also frequently have video feeds transmitted from remote units and helicopters. These feeds are relayed to the EOC to supplement broadcast reporting with additional footage.

F. Commercial Service Providers operate the familiar cellular Telephone service. The structure of their protocols provides geolocation from base station sector directionality, or in some cases, by GPS coordinates derived within the call phone or mobile units. As highway coverage is an important revenue source, the cellular providers have good coverage in high-density traffic areas. The resulting data has a characteristic pattern of sector utilization and hand-off that changes when traffic disruption occurs. When traffic is congested or blocked, the resulting data can be analyzed and overlaid on local GIS data to assist in dealing with the vehicular congestion described in Event 13. Delivery of that information is over the carrier's existing data service connection.

G. Connection between the city EOC and ITS will be by landline. Relevant data is then forwarded to the incident command post by their RF link. Intelligent Transportation System

(ITS) support data for emergency vehicles in movement is transmitted direct between the vehicle and the ITS infrastructure; emergency vehicle priority in the ITS system supplements Code 3 operation.

3. **Procedural**: Procedures for incident management vary significantly as incident commanders tailor response to local conditions. As additional sensor output is provided, there is danger of data overload both in terms of overwhelming the communications resources and in overloading the human decision makers. Data processing facilities in IC, supplemented by those in EOC, reduce the data load by eliminating redundant or unchanging information reports, and by well-designed data presentation on computer displays. Training in display management for IC personnel is needed to optimize decision-making.

   The sensor data stream is in parallel with voice communication. Legacy operating procedures may need to be extended to ensure that all personnel have the same context for understanding full implications of information derived from sensors.

   With access to data transmitted from sensors located in responder PPE, and facility mechanical systems, commanders can warn firefighters where toxic or over-temperature conditions occur. For example building fan controls can be used to reduce oxygen delivery or control air pressure within parts of a structure.

   Availability of significant amounts of visual information from video footage enhances understanding of the scene, but also presents a problem of viewing time required. The addition of video backup and storage in the better-equipped and environmentally controlled city EOC partially addresses the need to immediately analyze real-time video with a high information density. It does introduce the need for on-scene personnel to request images of specific areas or events. Protocols must be established for its delivery to the scene with the video, plus contextual and interpretive information so there is no confusion about what the images are showing.

4. **Regulatory**: Regulatory agencies are sensitive to the needs of PS agencies, and a number of actions are being proposed and implemented. Priority access to commercial capacity can be required to accommodate emergency response traffic. 700 MHz or 4.9GHz FCC licenses in the US can provide needed bandwidth and useful air interfaces with appropriate priority structures. Unlicensed operation in Whitespace TV spectrum can also support a number of applications for emergency response.

5. **Chronological**: Availability of sensor data might help reduce the need for a change in evacuation in Event 32. Otherwise, the timeline is not changed.

5.8.3.1 Functional Capabilities

Functions include the following:

- Enhancement of cognitive radio functionality to improve PS systems and within systems that are sources of data to automate handling of the significantly increased traffic volume.
- Enhancement of PPE sensors, ad-hoc networking, pebble technology supplementing the incident area network, monitoring software in IC with cognitive tools to provide an effective display of current conditions and generate appropriate alarms.

- Prior planning with building personnel to establish details of connection to the building management and mechanical systems, and provisions for taking control.
- Process to monitor weather information continually in the city EOC, and procedures/standards that specify information format when it is relayed to IC.
- Video feed from traffic control center to EOC. Training for personnel to determine procedures/standards that specify what images & video information are needed, and what format is used when it is relayed to IC.

5.8.3.2 Regulatory Implications

Most of the communications described in this Use Case will involve use of spectrum that is already licensed. Permission may be needed for TV band use. Regulatory action may be needed to provide additional spectrum to construct networks with adequate bandwidth.

5.8.3.3 Policy Implications

In some cases PS planning is completed with the assumption that every resource utilized is brought to the scene by first responders, and controlled by them. Some of the items described above, in *5.8.3.1, Functional Capabilities*, may require changes in policies and procedures. For example, this use case would require:

- Accepted agreement with TV stations as to what services will be provided, technical details of channels to be used, and integration of that information into incident response equipment, procedures, and training.
- Accepted agreement with cellular service providers as to exactly what call traffic data can be made available, and in what format. Capture of that real-time data is a function of cognitive functionality within the cellular infrastructure. Provisions for protection of data, ensuring the privacy of individual callers must be addressed.
- Agreement must be reached between PS and DOT authorities as to what ITS traffic information will be exchanged and the formats to be used. Incorporation of CR capability in both systems to automate as much as possible of the information exchange process, and to define policies for its use. Training for control of the two systems when they are connected and procedures for disconnecting the systems.

5.8.4 Summary of Impact of Use Case

This Use Case describes a number of opportunities to enhance sensor information available during an incident. These capabilities are relatively independent; application of any of them has potential to improve operations. The case also identifies potential problems that may arise as a result of the sheer volume of data available. Cognitive Radios, and cognitive functionality in other areas of the system, can be of great assistance in reducing the volume of information transferred over the network and also increase its relevance for recipients.

An important consideration is how much of the decision space can be stated as policy, and delegated to cognitive functionality for execution. Insufficient delegation leads to individual overload, while too much delegation can result in inadequate control under unusual circumstances. Another consideration is the human-machine interface. Users must be able to vary the level of control they

want to retain, and the information they want to see must be in a form to facilitate decisions to be made.

Facilities such as we have described can provide better projections, and reduce the likelihood of unexpected developments. That, in turn, permits first responders and commanders to be more proactive and less reactive.

6 Additional Capabilities and Topics

There are several issues that must be addressed in support of most or all of the use cases defined in Section 5. These issues cut across specific applications of cognitive technology, and are relevant for any application of cognitive radio technology for the benefit of public safety. These issues include:

- Security;
- Auditing for purposes other than security;
- Interface to legacy systems and transition to cognitive capabilities;
- The interrelationship of use cases;
- The interrelationship of communications and information management; and
- Standards.

6.1 Security Issues applicable to and Capabilities Required to Support SDR/Cognitive Radios

Given the potential of SDR and cognitive radio technologies to reconfigure communications capabilities, a key consideration is to ensure that radios, and the systems of which they are a part, are protected from malicious commands to alter configurations or performance parameters and from attempts to disrupt communications. As such, security is a critical topic that applies to all of the use cases described in Section 5. Security discussed in this section is primarily limited to ensuring the integrity of radio system—not mission or operational security or security of the communications themselves. In other words, we focus on ensuring that the radio operations are protected from malicious attack.

In today's world of viruses, Trojans and other forms of malicious attacks are commonplace in computational environments, including those of software reconfigurable radios. In this hostile environment, security functions should reside at the top of the list of essential requirements for all SDRs, and especially cognitive radios. Some of the most important security functions are included in Table 2 and are discussed below.

Cognitive radio systems, because they learn about their local operating environment and alter their behaviors as a consequence of the environment, are potentially vulnerable to new forms of attacks; attacks which attempt to exploit and influence the behavior of the cognitive system in a way which is both detrimental to the behavior of the CR system and desirable to the attacker. Some of these vulnerabilities have been addressed in a Forum submission to the International Telecommunications Union (ITU) in a document published in September 2008[21]. An extract of this document is provided below in Appendix C, which includes the specific text from the report, addressing security concerns related to cognitive radio systems.

One potential attack not addressed in that submission is one in which the attacker, who is aware of the external parameters and factors which can influence a given CR system's behavior, attempts to influence these factors by altering the external environment in a manner that will, in turn, influence the behavior of the CR system. The specific methods and means employed by the attacker will be dependent on the actual behavioral characteristics of the CR system, thus we are not able to address

[21] *SDRF-08-R-0010-V0.5.0, Input to ITU-R WP5A on Cognitive Radio Systems, 2 September 2008,* available on the Forum website (www.wirelessinnovation.org) under the Document Library.

specific details concerning the attacker's methods without knowledge of the specific CR system behavior. The Forum's input to the ITU, included in Appendix B, does describe some methods, particularly those that might be employed by CR systems using "pilot channels". The key point to consider for any CR System is whether or not the planned cognitive behavioral characteristics are vulnerable to exploitation in this general manner. If such vulnerabilities exist, then the design of the system should be modified in a manner which mitigates or prevents any exploits.

Table 2: Essential Security Functions for Cognitive Radios

• Access control, including authorization for: o Software Downloads/Updates o Policy Downloads & Updates o Configuration Data downloads/Updates o Human-Machine Interface interactions
• Identification, authentication and non-repudiation services for: o Users o User Devices o Network Devices o Network & Other Service Providers o Software providers
• Information integrity for : o All resident user data o All resident radio & network configuration Data o Any downloadable data or software o Over the Air Control and configuration commands o All resident software and firmware
• Credential, certificate and key management services for: o Users Certificates and private keys o Device Certificates and private keys o Root & intermediate Certification Authority Certificates o PINs, Biometric access and other electronic credential data
• Confidentiality including encryption & decryption services for: o User communications o Network control communications o Software Downloads o Policy (security, regulatory etc.) downloads o Configuration Data downloads o Device Uploads to networks (e.g. Log data, configuration data) o User data Storage o Configuration Data Storage
• Auditing o Usage logs o Security logs o Cognitive Operations logs
• Security policy enforcement

As this report was being generated, the Forum's Security Working Group (SecWG) was concurrently preparing a document entitled "Securing Software Reconfigurable Communications Devices" which addresses these and other import security functions as well as fundamental design aspects that are recommended to be a part of any software reconfigurable radio. Especially important are design considerations regarding the overall security architecture for the radio. Many devices today provide some or all of the security functions listed in Table 2, however the underlying security ar-

chitecture in which these services are provided is either non-existent or fundamentally weak in design. Unless the security architecture exhibits robustness appropriate to the identified threats and their associated risk probability assessment, the security services, and the protection they provide, could be bypassed or otherwise compromised.

The above referenced SDRF SecWG document also contains an extensive list of design requirements that address the full spectrum of security functions. Future documents by the SDRF Security Working Group will employ use cases to develop recommended security profiles for different radio applications such as public safety, network infrastructure, user cellular handhelds, etc. The reader is urged to read this document when it is published (expected in the late 2009). Until such time the following section provides a brief summary of these services and examples of how they might apply in a cognitive radio system. The following section contains a condensed and edited extract of a portion of the SDRF SecWG document.

6.1.1 Access Control Service

Traditional access control includes defining who has access to machines using PINs or passwords and profiles which define individual user access rights/privileges. For Cognitive Radios and other system/network components, access control has a much broader context including authorization for who may authorize and distribute (download or update), software/ firmware download for either new functions or update to previously installed applications. Similarly this security service also applies to downloads or updates operations addressing machine interpretable policies (e.g. regulatory, security, etc.), as well as radio and/or network configuration data, radio environment mappings, and other information. Thus any information that can be loaded via the air interface or any other device interface should be subject to access restrictions which define who is authorized to perform the associated function, the authenticating authorities, and span of their authority. In some instances, for very security sensitive operations, the definition might require preloading of digital credentials of authorized individuals, while for other less sensitive operations the authorizations might be contained in downloadable policies.

Access control measures may also be applied to components of the communications system. Such measures could prevent lost or stolen public safety radios from being used to monitor communications or from attempts to spoof operations by false communications. Access control of this type could essentially lock out these radios. Likewise, access control applied to network services and operations could help prevent misuse or fraudulent activities involving these assets.

In extremely sensitive radio applications (e.g. public safety, homeland security and other federal agency applications) which are at high risk of malicious software code attacks, access control measures might also apply to internal software operations by defining which applications can use specific services, which have data read and or write access rights, etc.

For a design viewpoint, determining which aspects of access control are applicable in a given application can only be determined by completing a comprehensive threat analysis and risk assessment which quantifies the likelihood (probability) that someone is willing to devote the necessary resources to attempt to exploit a perceived vulnerability.

Public Key Encryption

For these digital forms of identification, the current technology involves the use of digital certificates which have been prepared, issued and digitally signed with a secure digital signature by a Certification Authority (CA) or a designated sub-authority. This technology uses an asymmetric encryption technology known as Public Key Encryption. Associated with each PKE Certificate issued to a user, a user device or other entity is a public key and a password/PIN encrypted private key. The public key is embedded into the certificate contents and thus is protected by the secure digital signature placed on the certificate by the issuing authority. The public and private keys are mathematically related in that information encrypted in the private key can be decrypted by the public key and vice versa. A private key signature allows the recipient to be sure that the document came for the originator and has not been altered in transit across the network. The digital signature forms the basis of authentication. To be sure that the sender is who they claim to be, the recipient can authenticate the certificate of the originator since it must have been signed by a CA or designated sub-authority, by using the public key of the CA to verify the signature on the certificate. This requires the authenticating device to have copies or the certificates issued to the CA and any other sub authority. The CA certificate in known as the "root" certificate since it is the anchor of "the chain of trust".

When it is important to document the occurrence of an event (e.g., logging into a database with law enforcement sensitive data) the device can record the event along with the entire digital certificate of the entity logging in as well as the document and/or token signed by the entity. The token is a piece of data (e.g., random number) produced by the recipient which is signed in real time by the entity logging in. This method prevents someone from impersonating the entity logging in. This record can then be used to counter any claim by the entity (who may attempt to repudiate the event) that the event didn't occur, or that even if it did, that the entity was not responsible. This results from the simple fact that only that entity could have signed the document/token when the transaction occurred. This is known as a non-repudiation service and is important in many types of transactions such as downloads into SDR devices or in financial transactions involving the user of an SDR or other computational platform.

6.1.2 Identification, Authentication and Non-repudiation Services

Access control functions are predicated on the ability to identify a user or entity (e.g. Network server) and to have some degree of confidence that the user/entity is who they claim to be. Identification is necessary for the users, their devices (e.g. the SDR), network devices such as servers, as well as organizational entities such as Software providers, Network Operators and the entire range of service providers accessible via wireless devices.

In simple systems users identify themselves with a user log-on name and enter a PIN or password. The PIN/password sometimes is the only thing entered and serves both as an identifier and "authenticator". Other means of identifying individuals include ergonometric information such a fingerprints or retinal scans of the eye. However, these ergonometric forms of identification of don't apply to the myriad of other types of entities who need to access systems via the internet or over the air interface. For individuals, digital devices containing electronic credentials are used. Among these are included RF ID devices, smartcards or other digital token devices.

6.1.3 Information Integrity Service

In the preceding section we stated that the digital signature process, besides permitting authentication of the source, also allowed the recipient to verify that the document had not been altered. This is possible because the digital signature process involves computing a mathematical function known as a secure hash (see for example FIPS publication 180-2).

The hash is computed using the contents of the document/token and a key (random number) created by the originator and is a form of encryption that produces a result that is signed by the private key of the originator. (This means that only the originator could have created the hash). The hash algorithm ensures that it is not possible to make alterations in the data being protected in such a way that the same computational result would occur, nor

Transport Layer Security

Many of us are also familiar with using secure communications for commercial transactions via the internet. These transactions typically employ a protocol known as Secure Sockets Layer (SSL) (also known as Transport Layer Security [TLS]) which uses the same PKE algorithms and certificates discussed earlier. Other protocol rely on another form of encryption known as symmetric key encryption using algorithms such a DES and AES among others.

In symmetric key encryption, all parties involved share a common private key. There is no public key in this system, only the private key. One presumed disadvantage of symmetric key encryption is the fact that the private key has to be distributed to all of the parties involved and it has to be done in a way that does not allow the value of the key to be compromised. In this instance PKE presents a solution which allows the private key to be securely distributed. In fact many internet transactions use this aspect of PKE unknowingly. This is due to the fact that the PKE algorithms are computationally intense and time consuming. To encrypt a full message or document intended for one or more recipients can be time consuming, particularly when multiple recipients are designed since the message would have to be encrypted separately in the public key of each, and each would then have to decrypt its own version of the message using its private key.

Instead, the originator generates a temporary private key and uses it to encrypt the message. Then it encrypts just the private key in each of the public keys of the recipients. It sends the one encrypted copy of the message and the encrypted private keys for each recipient to all intended recipients. Each recipient then decrypts its copy of the private key, and uses it to decrypt the message. Thus in this case PKE is being used as a form of key management.

The use of encryption to protect communications in transit is perhaps the most commonly viewed use of this technology. These communications may be to encrypt voice communications or sensitive data (e.g, financial, medical, legal) or to protect the intellectual property of it creators (e.g software). For some information, encryption is necessary not only while it is being communicated between two or more points, but also when it is in storage. For example, users may wish to store passwords and other personal/financial data on their communications device.

could any other data combination provide the same result. This guarantees that data cannot be altered without detection, nor could an entire document be substituted. The recipient can then use the same key (which has been provided in the transaction) to calculate the hash and compare it to the value included in the signature (which has already been authenticated.) The recipient thus determines that no alterations have occurred.

This same technique can be used to protect sensitive data stored within the SDR as well as for any software downloaded into the device. It can even be applied to commands sent over a control channel used to control and manage the SDR.

In some especially sensitive applications, it might be applied to firmware and software stored on the SDR to ensure that the device has not been tampered with.

6.1.4 Confidentiality Service

The confidentiality service is often one of the first that comes to mind when one thinks about security. Many of today's commercial wireless systems employ some form of privacy, particularly for the air interface, but these methods are limiting in that they only protect the air interface portion of the larger communications path and some have proven to have exploitable weaknesses, most notable the WEP encryption initially used on WiFi links which has been superseded by WAP and WAP2.

What is important to emphasize is that because true end to end encryption is not always the case in the commercial telecommunications world, if the data is really sensitive and needs to be protected, it should be encrypted only at the source and decrypted only at the recipient. Furthermore if the data needs to be protected in storage, then the entity storing the data should encrypt it using a privately generated (symmetric encryption) secret key which it then protects by encrypting it with its PKE public key which can only be decrypted using his private key.

Before leaving this topic, it is important to note that in the PKE system, the private key is itself encrypted using a password issued by the Certifica-

tion Authority or its designee. Thus the password is a form of encryption key, When humans are involved, it is the responsibility of the human to protect this password. However, there are many computational entities, including SDRs which use PKE, and they must possess their own digital credentials.

For these devices, the manufacturer of the device must provide an answer to the question- how is the password for the device's private key to be securely protected? One recognized approach is to build into the device a tamper resistant secure storage area only accessible by the device when power is applied. Another, less desirable method would be to require the user of the device to enter this information via the device's keypad, while a third alternative would be to store a part of the password in a removable storage device kept by the user and required to be available to the SDR when power is restored. Other methods may also be employed.

6.1.5 Auditing

Auditing is a security service which records events to permit subsequent analysis of the events. Some of the events which may be recorded relate to security such as user log-ins (who and when they log in or are logged out), others events may relate to radio usage (start time, duration and channel used), radio management (e.g. download events, configuration changes) or for a CR a record of cognitive operations, which might include recording of location, channel usage and parameters which effect cognitive decisions.

Auditing is considered a security service because the integrity and accuracy of the events logged must be maintained and protected from accidental or intentional attempts to alter the log. Furthermore, access to the log needs to be restricted to authorized individuals for user privacy as well security concerns.

Because of limited storage for many, if not most, wireless devices, frequent uploading of the log to a central repository would be warranted. For these uploads off-line encryption would be used to encrypt the information before it is transmitted. If PKE is used, the public key of the device controlling the central repository would be used to transmit a copy of the symmetric key used to encrypt the log. Only the repository device would be able to decrypt this key and use it to decrypt the log contents.

The wireless device would also be required to provide a secure digital signature and integrity hash for the log contents prior to uploading. This validates the source and the integrity of the log contents and should be maintained along with the original log content in the central repository as long as the log data is retained. That may then be used to provide non-repudiation services.

Depending upon the specific radio application it might also be relevant to encrypt the audit log records while in local storage in the wireless device to ensure that privacy is not compromised should the radio be lost or stolen.

For an SDR there may be value in being able to configure via a data or policy download, which events are to be recorded in the audit log and the frequency or times when the log is to be uploaded. Being able to select the specific events allows not only for controlling storage needs and uploading frequency, but it also permits focused study of events with subsequent off-line analysis, or tailoring the log to the specific application for which the radio is being used.

6.1.6 Security policy enforcement

Before addressing security policy enforcement it is relevant to understand what is meant by the term "security policy". In fact there are several meanings depending upon your perspective.

An Organizational Security Policy (OSP) is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide. It is a document external to the SDR and is enforced by the individuals in the organization.

A System Security Policy (SSP) s a set of rules and practices that specify or regulate how a system provides security services to protect resources. The SSPs are thus components of Systems security architecture and design. Significant portions of the system security policies are implemented via security services and employ security policy expressions and/or are built into the system design. The SSP should implement relevant aspects of the Organization Security policy.

An SDR Platform security policy is a set of rules, either implicit in the design and/or explicit via machine interpretable expression, which define and limit the application of security services and to govern or restrain a system's possible actions as defined by the System Security Policy.

As a practical matter there may be multiple entities that supply SDR Platform security policy but there will be one entity that defines the overall policy including the authority given to other entities. It is incubating on that entity that it ensures the delegated authority does not lead to conflicting policies or that when conflicts arise it provides a means to resolve that conflict.

From these somewhat codifying definitions, it should be clear that it is not possible to design a radio that has any security enforcement without first defining the first two levels of the security policy because they generate the SDR security policy which the design must enforce. This policy clearly has a significant impact on the SDR security architecture and the implementation and design governing how the various security functions and services will be provided.

6.2 Auditing for Purposes Other than Security

In addition to the importance of auditing from a security standpoint as addressed in Section 6.1.5, there is a need for auditing purposes to support additional requirements. Auditing is important to provide:

- A record of the basis of decisions within the radio system for post-incident analysis.
- A record of the basis of decisions to improve and enhance cognitive radio capabilities.

Cognitive capabilities by definition include a significant number of decisions made at the subscriber radios and within network operations—more decisions than can be made by human operators. The power of cognitive radio is the ability to make such decisions in a rapidly evolving environment. Given the dynamic nature of the communications environment of incident response, some decisions may be counter-intuitive or may result in suboptimal network performance. The real time capability to manage such situations is based on human oversight of the network operations and the requirement to rollback changes that do not result in desired outcomes. To supplement real-time control of the system, it is also useful to analyze the performance of cognitive networks after an incident to understand the decisions that were made. Thus an auditing capability is an important component of the system. Information regarding cognitive radio decisions should be recorded for post-incident analysis.

There are a number of tradeoffs in the implementation of this functionality. Subscriber equipment, particularly portable devices, is limited in terms of the storage available for audit information. Storage requirements can be reduced by uploading data, but uploading then consumes spectrum that may be needed for critical communications during an incident. Storage is more readily available within the network infrastructure, but computation cycles devoted to storing data for subsequent analysis are then not available for real-time network operations. Thus the critical tradeoff is determining the value of data stored for subsequent analysis versus the costs (in terms of memory, communications, and computation) of recording the data.

One approach to the tradeoff is to allow modification of the type of data that is logged. For example, more data could be logged during a training or test exercise, while a minimal amount of data would be logged during real-time operations. Another important aspect of this capability is a set of tools for efficiently analyzing the data.

6.3 Transition and Interface to Legacy System

Realization of any of the use cases described in Section 5 will not happen "overnight" even at the point where the technology is proven, supporting regulatory changes have been instituted, and policies and procedures have evolved accordingly. Thus in each use case functional capabilities, regulatory considerations, and policies and procedures will also be needed to accommodate legacy systems.

The use cases postulate cognitive capabilities at some point in the network; the challenge is the interface between a network that has cognitive capabilities and legacy subscriber equipment (and networks). Specific functional capabilities within a cognitive network required to accommodate legacy systems include the following:

- The ability to distinguish legacy equipment and the capabilities of each device. Note that since legacy equipment may not be able to provide sufficient information about itself to the network, it may be necessary for the network to recognize the waveform characteristics and derive/infer the device capabilities.
- The ability to reconfigure transmit/receive capabilities to interface with legacy equipment and bridge as appropriate to establish necessary communications with other subscribers on the network.
- The ability to establish/re-establish communications links to avoid interference to/from legacy equipment.
- An appropriate subset of these functional capabilities may also be implemented within subscriber equipment that has cognitive capabilities.

6.4 Interaction of Use Cases

While the preceding use cases have been described and analyzed independently, there are interactions among the use cases and the cognitive capabilities that support these use cases. For example, dynamic spectrum access and dynamic prioritization could interact such that responders with the highest (or lowest) prioritization could utilize dynamically allocated spectrum to maximize access for the highest priority users. Secondly, dynamic spectrum access techniques may be useful in realizing the network extension use case. Network extension capabilities could be used to link to non-

first responders. Finally, we also recognize that the issues of command and control described in Section 5.2 become even more challenging as capabilities are implemented to realize multiple use cases.

It is beyond the scope of this report to address all of the issues that could arise in the interaction of use cases, so we simply note that there could be additional interactions to consider in addressing multiple use cases, in terms of functional capabilities, regulatory considerations, and policies and procedures.

6.5 Interrelationship of Communications and Information Management

Cognitive radio functions are a subset of cognitive capabilities used to maintain the safety of both the general public and the first responders who protect them. Cognitive radios support communications needs through the allocation of resources that support the command and control functions necessary to effectively respond to an incident. Efficient use of network resources to optimize incident response requires not only capabilities to optimize use of communications resources (i.e., to move the optimal amount of information) but also capabilities to ensure delivery of the most important information. Designating the relative importance and priority of information being transmitted goes beyond the scope of just the communications system. The applications that produce or consume the information ultimately determine the information priority.

However, applications that produce/consume information, and the communications capabilities that transport that information, must work cooperatively to ensure that that first responders and incident command have access to the most critical information when it is needed. For example, graceful degradation of video quality in response to bandwidth constraints is most effective when the application producing the video, the application using the video and the communications system work synergistically so it can degrade it in a manner consistent with available communications capacity while maintaining the ability to fulfill incident management needs.

In several of the use cases, we identify cognitive capabilities that would likely go beyond the scope of the communications system itself to include capabilities of sensors, command and control applications, and so on, that utilize the communications capability. Because of the synergistic aspects noted in the preceding paragraph, we have not attempted to make a precise distinction between cognitive capabilities incorporated into cognitive radios and cognitive capabilities of the applications that consume the data that is supplied via the communications system.

6.6 Standards

Some of the use cases involve communication of control information among subscribers (e.g., discovery of peer radios) or between the network and subscribers. Examples of the latter include information concerning roles and priorities. There needs to be standard protocols for the transmission of such information to ensure that radios are interoperable.[22] The specific protocols requiring standard definitions will depend in many cases on the specific approach used to implement functional capabilities identified in the use case, so it is important to recognize that standards will be needed to ensure interoperability of cognitive radios.

[22] Recent legislation passed by the U.S. Congress requires that federal grant money can only be spent for communications equipment developed pursuant to voluntary consensus standards where such standards exists.

7 Summary

7.1 Summary of Functions and Capabilities

Each of the use cases described in Section 5 requires certain functions and capabilities to be implemented. In this section, we restate these functions and capabilities in a summarized list. This list documents the technical challenges and research areas in cognitive radio that we have identified through this use case analysis.

Cognitive radio functions required to realize this use case include the following (the numbers following each function/capability map back to the number of the use case(s) in which the requirement for the functional capability is identified:

- Explicit definition of user roles within an incident response structure. [1, 6]
- Electronic storage of a user's credentials. [1, 6]
- Ability to authenticate a user as qualified for a specific role. [1, 6]
- Ability to query radios for information including, but not be limited to, vendor, radio type, available modes, version numbers, reconfigurability, etc. [1, 6]
- Definition of appropriate radio capabilities as associated with a user's role. [1, 6]
- Ability to associate users, radios, and user roles. [1, 6]
- Ability to reconfigure the radio based on the user's role. [1, 6]
- A standards-based over the air programming capability to include the software tools and "meeting point" (standardized modulation, bandwidth, frequency, and protocols) configuration. [1, 6]
- Sufficient security to ensure integrity of the over the air reconfiguration process. [1, 6]
- Ability to restore the radio to a previous configuration including a default configuration and the configuration of the radio prior to the incident. [1, 6, 8]
- Ability for individual radios to provide some information about the RF environment at their location, and a standard method for transmitting this information back to the network for analysis. [2, 3]
- Ability to identify the geolocation of network nodes. [2, 3, 4]
- Ability to monitor, anticipate, and identify network resource allocation issues. [2,3]
- Ability to adjust spectrum utilization based on defined policy (such as a network sharing agreement). [3]
- Ability to release use of spectrum by public safety users as the emergency communications requirements decline. [3,8]
- Ability to allocate additional spectrum in the most effective manner. [2,3]
- Ability of each subscriber to specify, to the network application, the subscriber units' data rate needs for its next transmission or message sequence. [4]

- Ability of each subscriber unit to rapidly change transmit power, waveforms, frequencies, filtering, and receiver attenuation based on commands sent over the network. [4]
- A network application that includes
  - A coverage and interference model that can predict signal and interference levels at every potential location of subscribers.
  - A CR algorithm that optimizes the following variables based on predicted signal and interference levels for all subscribers:
    - Transmit power
    - Waveform for communication (various bandwidths corresponding to different data rates)
    - Frequency channel(s) for communication
  - Dynamically controllable access priority per subscriber unit [4]
- The ability to set up an ad hoc network[23] [4]
- Ability for externally adapt and/or control antennas for the sites and/or terminals that can place additional gain in the direction of the desired communications and/or nulls in the direction of interference sources. [4]
- Ability to identify operating parameters of communications links to be connected. [5, 6]
- Reconfigurable multiband radio modules that are components of the gateway device. [5, 6]
- Ability to identify the degradation of performance, "ping pong effects" when communicating with a repeater, situations in which a channel is "locked up" due to improper parameter setting, etc. [5, 6]
- Ability to pass authentication and credential information from one system to another through the gateway. [5, 6]
- Ability to recognize when a reconfiguration results in a degraded capability. [7]
- Ability to store configuration information. [7]
- Ability to restore a configuration. [7]
- The protocols and algorithms to ensure that all radios rollback to the same known and valid configuration. [7]
- Ability to return to a default configuration via over the air command or reprogramming. [7]
- Ability to automatically handle significantly increased traffic volume. [3, 8]

[23] See Use Case 1, Section 4.3.1., "Use Cases for Cognitive Applications in Public Safety Communications Systems Volume 1: Review of the 7 July Bombing of the London Underground," Report No. SDRF-07-P-0019-V1.0.0, 7 November 2007, available at www.wirelessinnovation.org.

- Ability to provide an effective display of current conditions and generate appropriate alarms. [8]
- Ability to access building maintenance systems. [8]
- Ability to monitor weather and environmental information and transmit to Incident Command and other network nodes as needed. [8]
- Ability to transmit video feed and/or other traffic and transportation data from traffic control centers and/or traffic sensors to network nodes as needed. [8]
- Accepted agreement with TV stations as to what services will be provided, technical details of channels to be used, and integration of that information into incident response procedures and training.
- Accepted agreement with cellular service providers as to exactly what of their call traffic data is to be made available. Selection of that data in operation is a function of cognitive functionality in the cellular infrastructure. Provision for protection of privacy of individual callers.
- Agreement between PS and DOT authorities as to traffic information to be exchanged and formats to be used. Incorporation of CR capability in both systems to automate as much as possible of the information to be exchanged, and policies for its use. Training in control of the two systems when they are connected. Procedures for disconnecting the systems.

7.2 Summary of Regulatory Issues

The previous use cases illustrate that there are regulatory implications to realize the full potential of cognitive radio. Regulatory needs across all use cases tend to fall in the following major categories:

Category 1 - Dynamic expansion of spectrum for already licensed first responders

Three of the Use Cases- 1, 2, and 8- had the common regulatory need of new licensing methods to enable radios from one jurisdiction to roam to another and be able to operate on the new jurisdiction's frequencies, and possibly with new operating modes for which the radios are not FCC certified.

Use Case 2 also considered "borrowing" frequencies from one jurisdiction for the sites and terminals on another that normally does not use these frequencies nor is licensed for their usage. This scenario is complicated by the strict frequency coordination normally employed via contour mapping and such to mitigate inter-system RF interference.

Use Case 3 involved allowing public safety operation of spectrum shared with another entity (such as a commercial network) if the need arises to increase system capacity.

Category 2 - Over The Air Downloads to Load Another Jurisdiction's Operating Modes

Use Case 1 also discussed how Role Based Reconfiguration capabilities could be greatly enhanced if the regulatory framework were in place to enable radios to receive over the air downloads of new capabilities, possibly using modes/modulations for which the radios have not been FCC certified. Also, there is work needed in the regulatory domain to enable "meeting places", which would include (a) frequenc(ies) where radios from diverse jurisdictions could receive

downloads for alternate modes/frequencies and security provisions to prevent downloads from unauthorized individuals.

Use Case 1 also considered the possibility of downloading the regulatory restrictions along with the radio code that could form a rule base to restrict the radios'

Category 3 - Enable other users to use public safety frequencies

As the converse to public safety's use of the spectrum of other entities (per category 1), Use Case 3 also considered the case where non public safety entities could use public safety channels on a shared public/private network. There are significant regulatory implications of the concept of a shared public/private network.

Use Case 6 considered a situation where unlicensed non-first responders could be allowed to use frequencies allocated for public safety service.

In both cases, regulations would need to be modified to explicitly define the circumstances and appropriate authorizations that should be in place to ensure that such communications is available when needed while not adversely impacting other first responder communications.

Category 4 - Streamlined radio certification regulations for expanded modulations and operating modes

Both Use Cases 3 and 4 described cognitive radio techniques that would more significantly exploit the SDR capabilities of modern-day public safety radios to dynamically change operating modes and waveform parameters such as bandwidth, data rate, transmit power, frequencies, antenna parameters, and type of modulation to balance/optimize loading and coverage. Since presently the amount (and cost) of testing needed for radio certification is directly proportional to the number of different waveform parameter combinations that the radio will use, such expanded capabilities warrant streamlining of the regulatory process for radio certification. Also, the same need applies to the licensing of the sites in a given system.

7.3 Summary of Policy & Procedures Issues

The cognitive capabilities of the above use cases generally impact existing public safety policies and procedures, summarized below:

Category 1: Linking of Radio Communications Capabilities with Rules

The linkage of communications capabilities with rules in Use Case 1 results is a need for new and revised policies and procedures that describe responders' roles and authenticate the users and their assigned roles.

Category 2: Training of All Levels of System Users

Almost all of the use cases may result in radios behaving differently than what has traditionally been the case for most existing systems, so training will be required so that users will know how to interact with the radio to use the enhanced capabilities for their maximum advantage.

Also, new CR capabilities such as those described in Use Cases 2 and 4 are a significant change in the role of the COML or network operations manager in terms of real-time network control. Current systems generally rely on extensive pre-planning, and network management generally ensures that the network stays operational. These use cases represent a much wider range of op-

tions for network resource management available to the COML or network operations manager, supported by data and analysis capabilities that are not available today.

Category 3: Radio Query Procedures

Some cognitive capabilities such as those described in Use Cases 1, 2, and 4 will require system queries of users' radios to ascertain their present capabilities. Procedures must be established for such queries, especially if they disrupt normal communications in any manner. Also, a standard definition of radio capabilities and the protocols for query/response must be defined.

Category 4: Policy and Procedures Harmonization for Disparate Systems

Inherent in many of the Use cases is greater reliance on other agencies or services than in the past, which necessitates varying degrees of harmonization of policies and procedures across these entities.

For example, Use Case 2 alludes to the possibility of combining resources of disparate systems (e.g., geolocation information) which necessitates cooperative sharing agreements for linking this information.

Use Case 3 for a shared spectrum partnership represents a significant challenge for harmonization of systems with significant, often seemingly incompatible, differences in policy and operating procedures into one unified policy/procedures agreement. Such an agreement would codify the policies of spectrum sharing.

Category 5: Circumstances and procedures for coverage and system resource expansion and rollback

Associated with Use Cases 2, 4, and 7 is the requirement that criteria be established to determine under what circumstances and how the CR techniques discussed therein be invoked for resource and coverage adjustments as well as rollback of such adjustments. These policies/procedures must include the definition of who has the authority to expand as well as roll back these capabilities.

Category 6: Circumstances and procedures for allowing users of another agency or service to communicate on a different system

This category embodies use cases where the "foreign" user is another first responder agency (Use Case 1), a non first responder entity (Use Cases 2, 5, and 6), or a partner in a shared network (Use Case 3).

7.4 Conclusions

Cognitive radio technology holds significant promise for improving and enhancing public safety communications capabilities. As described in this document, cognitive radio technology can allow a transition from today's concepts of a static communications capability to a dynamic capability that can be configured to meet the evolving demands of incident response. The result can be:

- Improved communication and coordination among first responders (not just the capability to be interoperable, but a communications capability that manages interoperability);
- Allocation of communications resources to meet the highest priority needs of incident response;

- Most effective and efficient use of the spectrum resources available for incident response, and the means to access additional spectrum when needed.

In order to realize these improvements, effort and investment is required to:

- Develop additional technical capabilities and functions;
- Address regulatory restrictions that impact the ability to implement those technical capabilities and functions; and
- Develop operational policies and procedures to harness the power of a more dynamic communications capability.

The definition of required capabilities in Section 7.1 forms a research and development agenda. The next step, which is being addressed by the Public Safety Special Interest Group, is to assess the maturity of technology with respect to those functional requirements, and to outline a roadmap for the development of technology that can meet the requirements. The regulatory considerations listed in Section 7.2 will be considered by the Forum's Regulatory Committee for future recommendations. The policy and procedural considerations listed in Section 7.3 will be addressed within the context of specific technology and regulatory developments.

To tie these threads together and provide an overall perspective of the role of cognitive radio technology, the Forum is also beginning a project, Information Processing Architecture (IPA), to develop a more detailed architecture based on this scenario (as well as use cases from other domains). This project will provide a general top-down model and a series of tools for depicting Operational, Systems, and Technical Standards Views of the structure of complex systems that will aid in defining, designing and selecting Cognitive Radio processes relevant and useful to Communication System stakeholders. Using a top-down approach will facilitate an improved understanding of the structure and relationships between Information Systems that span user domains, and allow users to assess the role of their systems with these architectural products.

A Acronym List

AP	Access Point
AV	All View (pg. 28)
AVL	Automatic Vehicle Location
COML	Communications Unit Leader
DOT	Department of Transportation
DPW	Department of Public Works
EM	Emergency Manager
EMS	Emergency Medical Service
EOC	Emergency Operations Center
EOD	Explosives Ordinance Disposal
FDMA	Frequency Division Multiple Access
HQ	Headquarters
IAN	Incident Area Network
IC	Incident Command
ICS	Incident Command System
IED	Improvised Explosive Device
ITS	Intelligent Transportation System
LE	Law Enforcement
LMR	Land Mobile Radio
MCC	Mobile Command Center
OFDM	Orthogonal Frequency Division Modulation
OV	Operational View (pg. 28)
PPE	Personal Protective Equipment
QoS	Quality of Service
RF	Radio Frequency
RFID	Radio Frequency Identification
SV	System View (pg. 28)
TDMA	Time Division Multiple Access
TV	Technical View (pg. 28)

B Extract from the Forum's Submission to ITU

Note: In the original Submission to the ITU the Forum's contributions were additions and suggested changes to an existing document. Thus the Forum's contribution text was high-lighted in the color blue. The following are relevant extracts applicable to the subject matter of this use case document.

Extract from Chapter 3:

"3 Security Considerations for Operational Cognitive Radio Networks.
While there are other potential areas which might employ such policies, cognitive radio node and network operations are likely to be driven by machine interpretable policy statements that are expressions which govern current security, regulatory, cognitive behavior and operational rules and restrictions. Each of these different types of policy is likely to be separately downloadable items since responsibility of their content is determined by different entities. For example, regulatory authorities define policies regarding regulatory aspects of operations and perhaps related security aspects. Service providers and network operators may use security policies to define aspects of download operations as well as operational constraints concerning aspects of cognitive behavior, while users might provide policy input regarding privacy of their data and communications.

There are a number of aspects related to these policies which should be considered and studied for standardization. These include:

- How many different policy types are needed (e.g., regulatory, network operations and terminal security, user security/privacy, cognitive terminal behavior, perhaps manufacturer defined policies regarding software downloads/updates)?
- How these requirements are expressed in a standard policy language in order that standardized implementations can be defined?
- Who creates the policies and how are the policies securely distributed and loaded into the terminal securely?
- What are the related integrity and authentication mechanisms used to safeguard the content of the policies, and how does a terminal determine who the authorized policy issuing entities are for each type of policy?
- How are regulatory and other authorities (including the user) assured that a cognitive radio node or network actually enforces the stated policies correctly?
- Is there a need for independent testing and certification entities and processes to certify compliance?

These are a few of the operational aspects which derive not only from cognitive radio aspects but also from the underlying software defined radio technology used to implement the radio platform. We shall discuss each of these in more detail. The security of these policies, maintenance, distribution process, expiration, are important to the robust operation of telecommunications and civil preparedness, and the approach to these issues can have significant benefit – cost ratio impact. Below, we discuss the design issues. However, it is readily apparent that for commercial telecommunications the complexity of policy management functions should be hidden from the subscriber terminal by performing as much of the cognitive functionality as possible at the base stations and within the network support at the base infrastructure.

8.3.1 Policy Languages

In the ideal case, the language used to express the rules expressed by any given type of downloadable machine interpretable policy should be defined and standardized. Whether the same language is used for all types of policy or whether each type has a unique expression tailored for the specific policy type is one aspect to be considered. Any such language must possess the capability for flexibility to be able to evolve as operational, regulatory and security needs change and evolve. The IEEE P1900.5 Working Group is actively studying this topic to develop relevant standards.

Standards in this area can significantly reduce terminal design complexity by avoiding the need for a radio node to implement multiple rules sets. Common standards also avoid the concomitant complexity required to certify that a terminal's operations properly conform to the varying policies. However, even with the use of standards defining policy languages, past experience with telecommunications security mechanisms recommends the use of strong integrity and authentication mechanisms to ensure that only valid policies from authorized sources are downloaded and implemented in a cognitive radio node. Thus the standards covering policies should include relevant security measures necessary to safeguard their content. Some recommendations for consideration are addressed in the next section.

8.3.2 Policy Integrity, Authentication and Verification

It has long been recognized that the processes for downloading software or policy into SDR platforms requires integrity and authentication mechanisms to minimize the threat of hacking SDR software. Even in an SDR software environment based on open standards, the barriers to hacking are fairly high because detailed knowledge of the terminal is required in order to produce code which can change terminal behavior. However, the use of a standard format to define operational policies regarding security, regulatory and other aspects of cognitive radio network operations could significantly lower the barrier of knowledge required and could ostensibly be viewed as increasing terminal vulnerability. The key to avoiding security weakness due to use of public standards is use of robust security mechanisms of encryption and authentication.

It is also essential to constrain who may actually author policy statements while also ensuring that the terminal receiving a policy statement will only accept it from an authorized source for the specific policy type. The definition of authorized sources for a given set of policies might itself be defined within another policy loaded by a service provider/operator. Included with the definition of the list of authorized sources and the policy types which each is authorized to author and distribute, should be the associated Digital Certificate containing their public keys. Each certificate must be able to be authenticated down the chain of trust to the Root Certificate. Because of global roaming, and very different areas of interest, a given terminal might actually have to support several different chains of trust, each relying on a different root certificate. Also due to the security critical importance of Root Certificates, each terminal should have a tamper-proof mechanism to safeguard the Root certificate(s) as well as any private keys used by the terminal for its security processes. Alternate methods of protecting root certificates are also available.

Robustness of these mechanisms varies in importance depending upon the type of network and role of the network node (e.g., commercial telecommunications, public safety, etc). Standardiza-

tion in these areas can simplify terminal and network design and operational complexity, and can permit the creation of independent certification authorities to ensure compliance with any relevant standards.

The integrity of all policies downloaded into a radio node must be maintained in storage, while in use, as well as after the radio power is turned off. This integrity can be maintained by storing the policy statements with locally applied integrity mechanisms, or by storing the policies in tamper proof storage accessible only to the security enforcement mechanism.

8.3.3 Policy Management Infrastructure

Historically, the creation of digital signatures and certificates necessitated the creation of a Public Key Infrastructure to support their use and distribution. Consequently, there exists a number of corporations around the globe who issue and manage digital certificates for public/business use. Similarly, the use of downloadable machine interpretable policies will also necessitate a Policy Management Infrastructure (PMI) to create, distribute, maintain and manage the relevant policies. The infrastructure could make use of existing PKI systems or incorporate similar yet independent capabilities within the PMI system itself or it may be that service providers/operators would establish their own PMI capability to service their subscribers. Regulatory bodies could employ these entities to distribute their policies or establish their own. Standards governing the establishment and required services may substantially simplify equipment design and operational harmonization.

8.3.4 Policy Conformance Testing and Certification

Consideration needs to be given to the manner in which conformance to any relevant standards or requirements is determined, regarding policy interpretation and enforcement/implementation by a cognitive radio node. For public/commercial applications, manufacturer self certification may be adequate, however for radios used for public safety/law enforcement, and other governmental applications, more rigorous methods should be considered.

For example, security requirements, policies and related implementations might undergo a certification process. Within this type of structure, different levels of assurance might be applied to the different cognitive radio applications. This form of certification would address the authentication mechanisms, storage and protection of the associated certificates, as well as protection of the integrity of the downloaded policies as examples. Similar or even the same methods might be applied to validate enforcement methods for regulatory and other types of policy.

8.3.5 Audit Logs

Audit logs are often viewed as a security mechanism and while this is a true statement, audit logs can also be used to provide other functions. In the context of cognitive radio systems, logs which record terminal behavior (transmission events including time and terminal location) can be used to assess cognitive radio network performance as well as review conformance to operating rules/policies. Such logs need not be maintained on the terminals for any length of time because they can be uploaded (after appropriate security measures are applied to ensure the integrity as well as non-repudiation of the content). Such a log might also be a means of identifying offenders who interfere with primary users and could be the basis for compensation to those users). However to be effective and to avoid proprietary implementations, standards for the recording,

uploading and the associated security measures used would result in a more effective system and allow simpler overall management and use of audit log contents. This would be particularly important if national regulatory bodies made this a mandatory function for cognitive radio networks

8.4 Authentication

Authentication and non-repudiation are recommended to be the foundation of most security functions employed by CR networks. Network operators would be assured that terminals requesting service were indeed legitimate users while mobile terminals would be able to authenticate that the CPC they are receiving is from a valid source and not a fraudulent source attempting to insert itself in the midst of a communication. Likewise as addressed in other sections and in Annex 3, authentication is essential for secure download of software updates, electronic policy statements and even economic transactions between a service provider and a user terminal.

Thus it would appear that authentication standards need to be established for global use across many different functions. This includes definition of the secure hash to be used for digital signatures, as well as relevant protocols to be applied. There are of course standards already existing in this area, but study and recommendation of those to be applied to cognitive radio networks would seem appropriate. It also may be necessary to develop new protocol standards for unique aspects of these types of networks.

8.5 Certification and Conformity

Some aspects of Certification and conformity are included in Section 8.3.4 and 8.16.1.3."

Extract from Annex 3 (to Annex 10 to Doc. 5A/45)
The Forum's Comments on the Cognitive Pilot Channel

"Security Considerations for Cognitive Pilot Channels

The benefits of a Cognitive Pilot Channel (CPC) may outweigh any negatives, but only if security measures protect the channel from adversarial tactics such as intentional jamming (potentially disrupting a public safety organization's communications), and spoofing (an adversary mimicking a CPC to misdirect and disrupt communications). Such attacks could derive from a variety of sources including criminal activities, terrorist activities, or malicious groups of hackers.

The specific countermeasures that may be most effective to mitigate such threats will depend upon the format of the air interface used for these communications. For example, the control channels of a CDMA system are protected by the unique spreading codes associated with each base station. This provides a measure of security and the existence of multiple base stations with overlapping coverage provide a form of redundancy to somewhat mitigate jamming. However, an adversary could have equipment which allows it to discover the codes being used and replicate them in attempts to "spoof" users into believing that the adversary is a legitimate base station and thus seriously disrupt communications.

Similarly the control channel of GSM networks is embedded into the multiplexed data stream, which makes it difficult for an adversary to mimic the behavior of the complete data stream. Rather than analyze all of the existing formats and since the format of the CPC has not yet been determined, we shall address general principles that can be applied when the CPC is designed.

B.1.1 Anti-spoof Measures

Perhaps the strongest measure against spoofing is the use of Public Key Cryptography to protect the integrity of the data while simultaneously providing assurance to the mobile terminal that the source of the pilot channel is legitimate. In this method, the pilot channel would periodically broadcast the content of its digital certificate (X.509) containing values which include its unique identifier and which defines its role as a CPC source. When received, the certificate can then be authenticated by the terminal through a chain of trust to a given root certificate using standard PKI authentication methods. The content of the CPC would itself not need to be encrypted (unless there is sensitive data which can be exploited), but each transmission block would carry a digital signature created by the CPC. Terminals could then authenticate the signature and thus validate the integrity of the data stream and the source. To guard against replay, the transmission should contain time of day information also protected by the signature.

This is perhaps the best method for preventing spoofing of legitimate CPC sources since it is completely independent of the signaling format of the air interface and employs robust but simple and straightforward security measures that are likely to also be used in support of secure downloads of policies and code updates to the mobile terminal.

Similarly, the terminals could use digital signatures on their transmissions in the uplink to validate and authenticate themselves to the CPC source, including a copy of their digital certificate

containing their public key in these transmissions. The certificate upload would only be necessary upon entering/re-entering a network since it could otherwise be distributed to other CPC locations or to base stations using the network infrastructure.

B.1.2 Anti-jamming measures to protect against denial of service

In the following discussion, the CPC is viewed as a logical or virtual channel independent of any given air signaling format. The CPC may become an essential component of telecommunications access. Specific CPC implementations may require different measures to diminish or preclude the effectiveness of jamming by terrorists or criminals. We shall thus limit our discussions in the main to general measures which should be considered until such time that CPC air signaling formats are defined.

In the commercial/civil domains the most effective measures against jamming are to raise the barrier to jamming so that jamming is either ineffective or infeasible. One way to raise this barrier is if the CPC is broadcast simultaneously from multiple sources with overlapping coverage. In this case, it becomes difficult to jam since each CPC source would have to be individually jammed. Thus, in CDMA networks each base station could broadcast a duplicate of the CPC allowing a terminal multiple opportunities to locate a legitimately usable channel.

Another possibility might be to broadcast the CPC downlink as a subcarrier on a commercial television channel. In this instance the CPC would contain information (frequencies, codes, etc.) that would allow the mobile terminal to establish a communications channel to a base station. The high power of the commercial TV broadcast by itself provides a strong measure of anti-jam protection and the fact that there are likely multiple TV stations broadcasting provides redundancy. These examples are intended to point out that methods are useful which raise the barrier to jamming by requiring a terrorist or criminal to use more resources to in their attempts to jam the CPC.

Of course, the design of the CPC coexisting within the signal format of the cognitive radio system may employ other anti-jam measures including coding, frequency hopping or other spread spectrum measures typically used on military systems. These techniques, however, can create complexity in the design of the overall system and increase synchronization times for terminals entering a new area of communications, as well as increasing terminal costs.

B.1.3 CPC Security Conclusions

We recognize that the cost and performance of specific measures to be used must be considered in view of the intended communications application (e.g., commercial, local/state public safety, federal/national public safety, etc.) as well as a risk and threat assessment.

The risk and threat assessment must consider the costs of the security measures being contemplated as well as assessing the risk and specific vulnerabilities of the planned CPC. Other costs and impacts that should be considered include the cost of recovery from successful exploits as well as the potential for loss of life or injury to individuals if the system is compromised or

jammed. This latter aspect may only be relevant when public safety, civil/governmental law enforcement or military communications are involved.

However, it will be important for the CPC to include authentication as a minimum since it will likely be part of the terminals' capability and is an effective means of providing anti-spoof protection. "